

QSC 2021 VMDR Overview

VMDR Training Documents

- QSC 2021 VMDR Overview Lab Supplement
- QSC 2021 VMDR Overview Slides

You can download both documents, just below the presentation you are viewing (at the bottom of the page).

Play Lab Tutorials

Navigate to the following URL to view the "Configure Agents for VMDR" tutorial

PLAY → <http://lor.ad/7bZE>

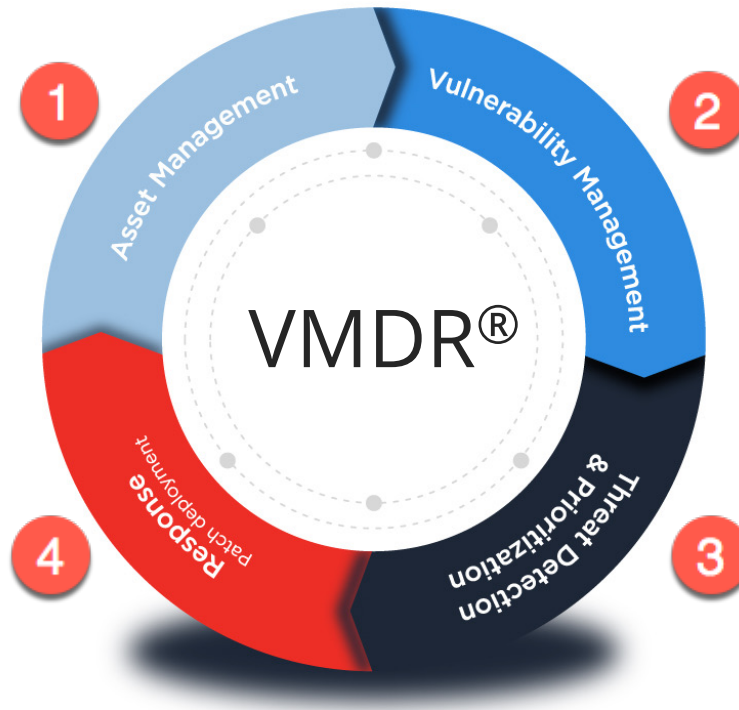
Click to open Lab Tutorial. 1

Maximize Screen 2

Click Start Button 3

The screenshot shows the Qualys Play Lab interface. At the top, there's a navigation bar with links: PRIORITIZATION, SCANS, REPORTS, REMEDIATION, ASSETS, KNOWLEDGEBASE, and USERS. The main content area has a dark background with a circular diagram in the center containing a play button. Below the diagram, there are three sections: 'Prioritize Threats' (with an upward arrow icon), 'Detect & Deploy Missing Patches' (with a gear icon), and 'Find all your IT assets' (with a magnifying glass icon). The 'Find all your IT assets' section includes a description: 'Discover, track and normalize asset information, including installed software and packages. Create dynamic tags, leveraging normalized data for grouping assets as and when they show up, based on intuitive rules.' Below this, there are two links: 'Manage Tags' and 'Visit Dashboard'. On the right side, there's a sidebar with a 'Try It' button, a red 'Q' logo, the text '15 steps / 3 mins', the title 'Configure Agents for VMDR', and a large 'Start' button. At the bottom of the sidebar, it says 'Nov 2020 by Qualys'. Three red callout boxes with numbers 1, 2, and 3 point to the URL, the maximize button, and the start button respectively.

Qualys VMDR Lifecycle



VMDR Agenda

1. Asset Management

- Qualys Sensor Overview
- CyberSecurity Asset Management (CSAM)

2. Vulnerability Management (VM)

- Vulnerability Findings
- Dashboards & Widgets

3. Threat Detection & Prioritization (TP)

- Threat Intelligence Feed
- VMDR Prioritization Report

4. Response – Patch Management (PM)

- Deployment Jobs
- Patch Catalog

Asset Management

CIS Control 1: Inventory and Control of Enterprise Assets



Overview

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.



<https://www.cisecurity.org/controls/inventory-and-control-of-enterprise-assets/>

Qualys Sensor Platform



APIs (collect data from 3rd parties)

Configure Agents for VMDR



- The patching and response functions in VMDR require Cloud Agent.
- Some Agent Activation Keys may need to be updated to include the VMDR application modules (i.e., VM, CSAM, SCA, and PM).

Lab 1: Configure Agents for VMDR

Please consult pages 3 to 13 in the lab tutorial supplement for details.



Tutorial begins on page 4.

10 mins

Upgrade Agent Activation Keys

Upgrade Agents with Activation Keys

VMDR requires the activation of a purpose-built engine for detecting missing patches for Cloud Agents. Select Activation keys which you want to upgrade for VMDR. All the agents associated with those keys will be upgraded.

Actions (1) ▾

Upgrade

Manage Cloud Agent Keys

1 - 2 of 2

	MODULES	AGENTS	TAGS
<div>Default VMDR Activation Key 28f4b0cd-f622-42e0-a809-c12474161c3f</div>	<div>Unlimited Key</div> <div>SCA VM PM CSAM</div>	0	-
<div><input checked="" type="checkbox"/> Minimum Module Activation Key 549c7a3f-fc20-44bf-8c54-e74f234b95d8</div>	<div>Unlimited Key</div> <div>CSAM</div>	0	VMDR Lab

- Upgrade Agent Activation Keys to include VMDR application modules (i.e., VM, SCA, PM, CSAM).

Activation Key Tagging Strategy

- **BEST PRACTICE:** Assign “static” tags to agent Activation Keys and use them to ensure agent hosts receive their appropriate performance settings, patching licenses, and patch job assignments.

The screenshot displays the Qualys Configuration console with the 'Licenses' tab selected. The 'License Consumption' section shows 'Patch Management' with a 'TRIAL' type and '10' licenses purchased. The 'New Activation Key' dialog is open, showing the 'Remote' tag selected for provisioning. The 'Include Assets Tags' section shows 'VMDR Lab' and 'Remote' tags. The 'Provision Key for these applications' section shows the following applications and their activation counts:

Application	Activations Remaining
CSAM (CyberSecurity Asset Management)	115
VM (Vulnerability Management)	15
SCA (Secure Config Assessment)	15
PM (Patch Management)	115
PC (Policy Compliance)	15

The 'Generate' button is visible at the bottom right of the dialog.

CyberSecurity Asset Management

Two Asset Management Applications

- **Global AssetView (GAV)**

Provides foundational inventory gathering capabilities for all assets in your IT environment, from on-premise servers and PCs, to Cloud instances, containers, Enterprise IoT and OT environments.











- **CyberSecurity Asset Management (CSAM)**

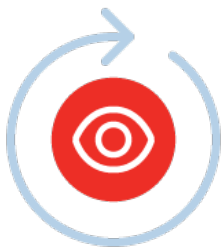
Delivers additional capabilities on top of GAV to provide users with cybersecurity related content, such as product lifecycle information, ability to define authorized and unauthorized software and integration with ServiceNow CMDB among others.



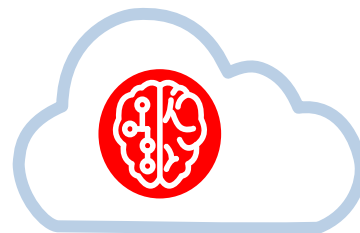
CSAM or GAV

KEY FEATURES		GAV (free)	CSAM
	Get complete visibility into your environment Discover and inventory all your assets	✓	✓
	View categorized and normalized hardware and software information Standardize your inventory	✓	✓
	Define criticality and find related assets Add business context through dynamic tagging	✓	✓
	Find and upgrade unsupported software and hardware Know product lifecycle and support information	X	✓
	Eliminate unauthorized software from your environment Quickly identify non-compliant assets	X	✓
	Be informed about assets requiring attention Receive notifications to review and define actions	X	✓
	Inform stakeholders about health of your assets Create custom reports	X	✓
	Easily keep your CMDB up to date Enable 2-way integration to sync with ServiceNow CMDB	X	✓

Comprehensive Asset & Software Inventory



Physical Scanner	Cloud Agent
Virtual Scanner	Passive Sensor
Cloud Connector	API
Container Sensor	Out-of-Band



CSAM Catalog: Categorize, Normalize and Enrich

OS/HW/SW	Lifecycle Stage
Support Stage	License type
Manufacturer	Category

- Qualys CyberSecurity Asset Management (CSAM) aggregates data from all sensors.

Qualys Categorization, Normalization & Enrichment

	Operating Systems	Hardware	Software
Raw Data	Base OS Runtime AIX: 06.01.0009.0300 EE	Dell, Inc. R510	mysql-community-server 5.6.35-2.el7.x86_64
Category	UNIX > Server	Computers > Server	Databases > RDBMS
Manufacturer	IBM	Dell	Sun Microsystems
Owner	IBM	Dell	Oracle
Product	AIX	PowerEdge	MySQL Server
Market Version / Model	6	R510	5
Edition	Enterprise	-	Community
Version	6.1	-	5.6
Update	TL9 SP3	-	35-2.el6
Architecture	64-Bit	-	64-Bit
Lifecycle Stage	EOL/EOS	OBS	EOL
End-of-Life	30-Apr-2015	1-Sep-2012	28-Feb-2018
End-of-Support	30-Apr-2017	1-Sep-2012	28-Feb-2021
Support Stage	Unsupported	Obsolete	Extended Support
License Type	Commercial	-	Open Source (GPL-2.0)



Normalization &
categorization



Advanced asset
information

Search Hardware Categories

hardware.category1: value1

hardware.category2: value2




hardware.category: value1 / value2



hardware.category1: `Networking Device`

hardware.category2: `Switch`

hardware.category: `Networking Device / Switch`

✕ hardware.category1: 'Networking Device'		
✕ hardware.category2: 'Switch'		
✕ hardware.category: 'Networking Device/Switch'		
ASSET	OPERATING SYSTEM	HARDWARE
10.46.105.2 10.46.105.2	 Cisco Systems NX-OS	Cisco Systems Nexus Switch Switch
10.46.105.1 10.46.105.1	 Cisco Systems NX-OS	Cisco Systems Nexus Switch Switch
10.46.105.3 10.46.105.3	 Cisco Systems NX-OS	Cisco Systems Nexus Switch Switch

Hardware Category List

CyberSecurity Asset Management ▾ HOME DASHBOARD INVENTORY

Managed ▾ **Assets** Software

MANUFACTURER

Amazon Web Ser...	11
VMware	8
Unidentified	5
Microsoft	1

TAGS

Internet Facing A...	17
Initech	13
AWS Ohio	12
Windows	11
AG: San Jose	9
11 more	↕

Group Assets by : Hardware Category ✕ ▾ 1 - 19 of 19

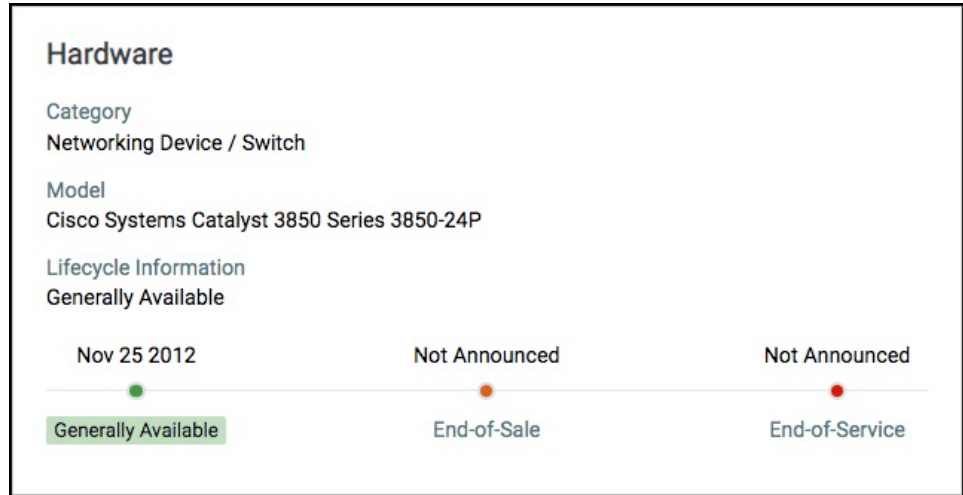
CATEGORY	ASSETS
Virtualized / Virtual Machine	589
Unidentified / Unidentified	238
Computers / Unidentified	238
Computers / Server	155
Networking Device / Unidentified	46
Virtualized / Cloud Instance	36
Network Security Device / Firewall Device	24
Networking Device / Switch	16
Unknown	14

- From the “Assets” tab, group assets by Hardware Category.

Hardware Lifecycle Stage

Search Token: `hardware.lifecycle.stage:` *value*

- **General Availability (GA)** - Hardware is in production, available for purchase, and supported
- **End of Sale (EOS)**- No longer being sold or by vendor
- **Obsolete (OBS)** - End-of-Service; no longer serviced via upgrades, patches, or maintenance
- **Intro (INTRO)**- hardware introduction date of interest



Search OS Categories

operatingSystem.category1: value1

operatingSystem.category2: value2

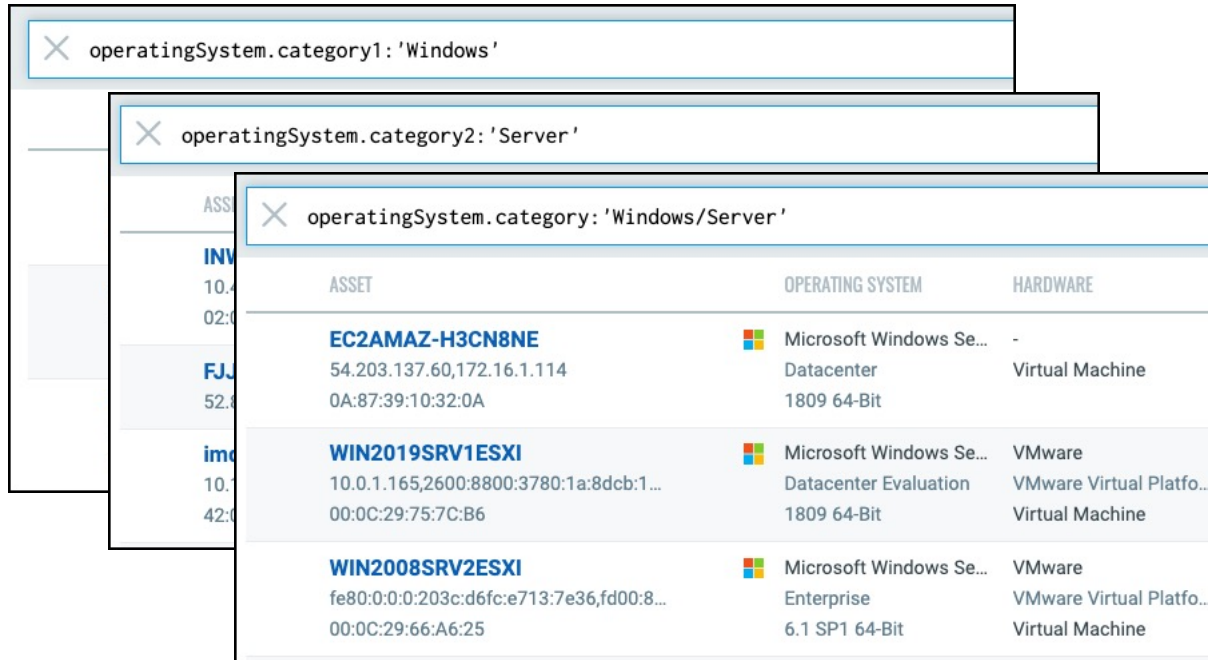
operatingSystem.category: value1 / value2






operatingSystem.category1: 'Windows'

operatingSystem.category2: 'Server'

operatingSystem.category: 'Windows / Server'



ASSET	OPERATING SYSTEM	HARDWARE
EC2AMAZ-H3CN8NE 54.203.137.60,172.16.1.114 0A:87:39:10:32:0A	 Microsoft Windows Se... Datacenter 1809 64-Bit	- Virtual Machine
WIN2019SRV1ESXI 10.0.1.165,2600:8800:3780:1a:8dcb:1... 00:0C:29:75:7C:B6	 Microsoft Windows Se... Datacenter Evaluation 1809 64-Bit	VMware VMware Virtual Platfo... Virtual Machine
WIN2008SRV2ESXI fe80:0:0:0:203c:d6fc:e713:7e36,fd00:8... 00:0C:29:66:A6:25	 Microsoft Windows Se... Enterprise 6.1 SP1 64-Bit	VMware VMware Virtual Platfo... Virtual Machine

OS Category List

The screenshot shows the 'CyberSecurity Asset Management' interface. The top navigation bar includes 'HOME', 'DASHBOARD', and 'INVENTORY'. The main header has 'Managed' and 'Assets' tabs, with 'Assets' selected. A modal is open, titled 'Group Assets by : OS Category'. The modal contains a table with two columns: 'CATEGORY' and 'ASSETS'. The table lists various OS categories and their corresponding asset counts. The background interface shows a list of manufacturers and tags on the left, and a table of assets in the center.

CATEGORY	ASSETS
Linux / Unidentified	329
Windows / Server	260
Windows / Client	231
Unidentified / Unidentified	203
Linux / Server	132
Network Operating System / Unidentified	89
Windows / Unidentified	32
Virtualization / Hypervisor Type-1 (Bare Metal)	29
Mac / Client	19

- From the “Assets” tab, group assets by OS Category.

Search Software Categories

software:(category1: value1)

software:(category2: value2)

software:(category: value1 / value2)



software:(category1: `Security`)

software:(category2: `Endpoint Protection`)

software:(category: `Security / Endpoint Protection`)

software:(category1: 'Security')

software:(category2: 'Endpoint Protection')

software:(category: 'Security/Endpoint Protection')

RELEASE	CATEGORY	LICENSE
Qualys CloudGuard 4.2.0.8		
Microsoft Windows Defender 4.18.1807.18075	Security Endpoint Protection	Commercial Free
Privax HMA! Pro VPN 4.6.151	Security Endpoint Protection	Commercial Licensed
OpenVPN 3.1.3	Security Endpoint Protection	Open Source GNU General Public

Software Category List

The screenshot displays the 'CyberSecurity Asset Management' interface. The top navigation bar includes 'HOME', 'DASHBOARD', and 'INVENTORY'. The left sidebar shows 'Managed' assets with filters for 'LICENSE' (Open Source: 145, Commercial: 52) and 'PLATFORM' (64-Bit: 45, 32-Bit: 1). The main content area is divided into 'Assets' and 'Software' tabs. The 'Software' tab is active, showing a 'Group Software by...' dropdown menu with 'Category' selected. A red arrow points to the 'Category' option in the dropdown. The main table displays the 'Software Category List' with columns 'CATEGORY' and 'INSTANCES'.

CATEGORY	INSTANCES
Network Application / Internet Browser	651
Application Development / Framework	594
Application Development / Development Tool	561
Networking / Access Software	464
Application Development / Programming Languages	443
Security / Endpoint Protection	442
Network Application / Web Servers	310
Databases / RDBMS	275
Security / Endpoint Management and Security	275

- From the “Software” tab, group software by Category.

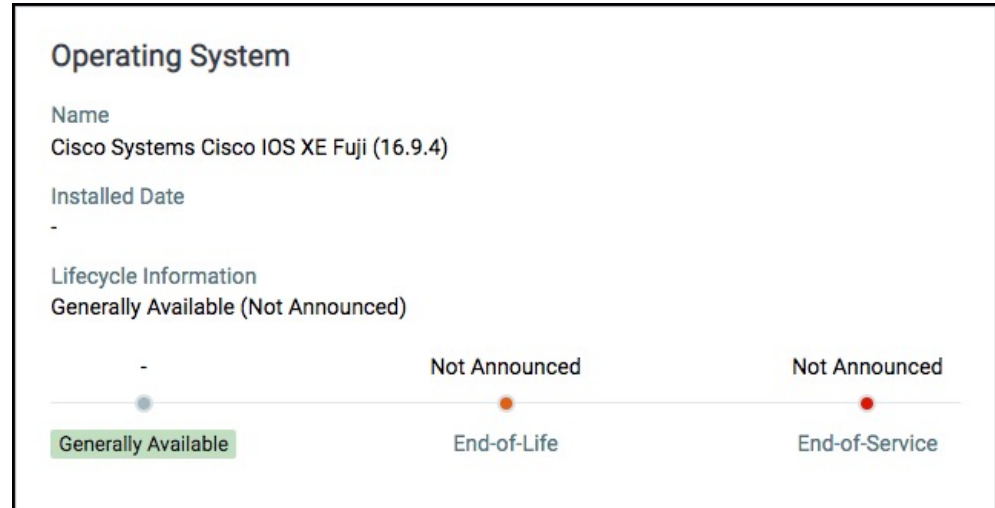
OS & Software Lifecycle Stages

Search Tokens:

`operatingSystem.lifecycle.stage: value`

`software:(lifecycle.stage: value)`

- **Generally Available (GA)** - When the product became available for purchase.
- **End-of-Life (EOL)** - No longer marketing, selling, building new features, or promoting product (Security patches may still be provided).
- **End-of-Service (EOS)** - No longer serviced via upgrades, patches, or maintenance.



Lab 2 : Search Using Categories

Please consult pages 14 to 15 in the lab tutorial supplement for details.



Tutorial begins on page 15.

5 mins

Software License Category

Commercial – Supported by vendor.

✕ software:(license.category:'Commercial')

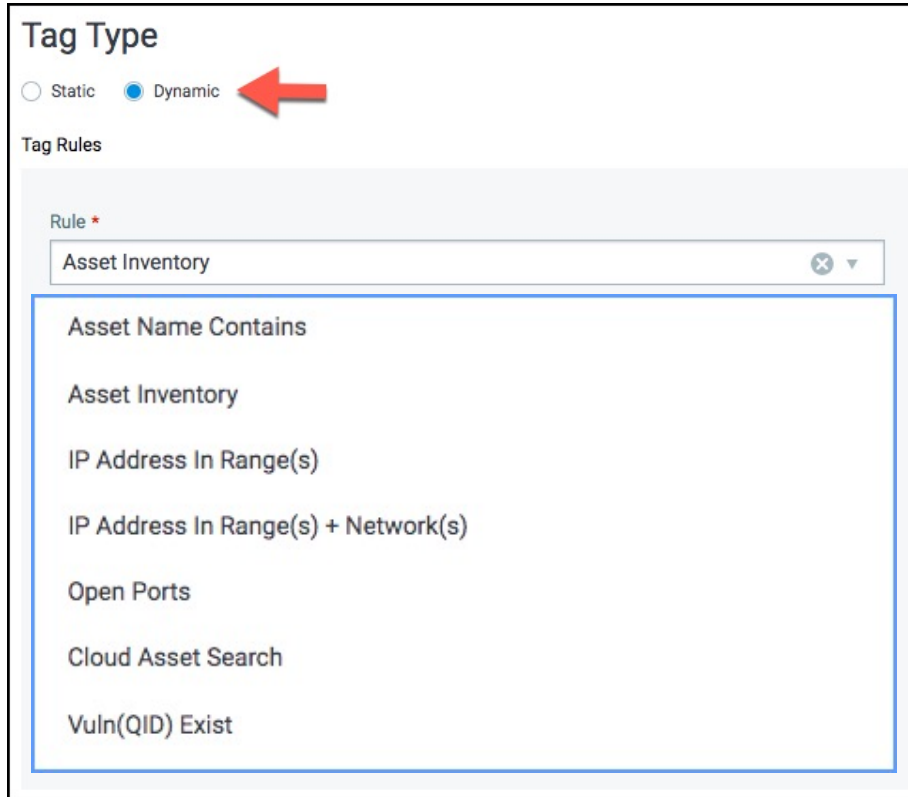


Open Source – Free for public use.

✕ software:(license.category:'Open Source')



Dynamic Rule-Based Tags



Tag Type

☐ Static ☒ Dynamic

Tag Rules

Rule *

Asset Inventory

- Asset Name Contains
- Asset Inventory
- IP Address In Range(s)
- IP Address In Range(s) + Network(s)
- Open Ports
- Cloud Asset Search
- Vuln(QID) Exist

- The “Asset Inventory” rule engine allows you to build tags using query tokens, including the Hardware, OS, and Software category tokens.
- Other “dynamic” rule engines are also available.

Lab 3 : Dynamic Rule-Based Tags

Please consult pages 16 to 17 in the lab tutorial supplement for details.



Tutorial begins on page 16.

5 mins

Unidentified vs. Unknown

Some OS and Hardware assets may appear as “unidentified” or “unknown.”

Unidentified

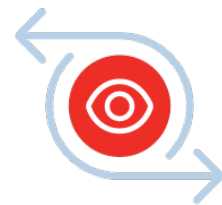
- Not enough data has been discovered/collected for Qualys to determine the asset’s hardware or operating system.

Unknown

- Adequate data exists for Qualys to categorize the asset, but it has yet to be cataloged.

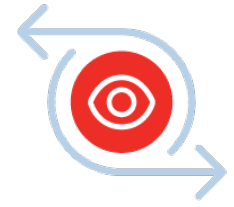
Network Passive Sensor

Passive Sensor Overview

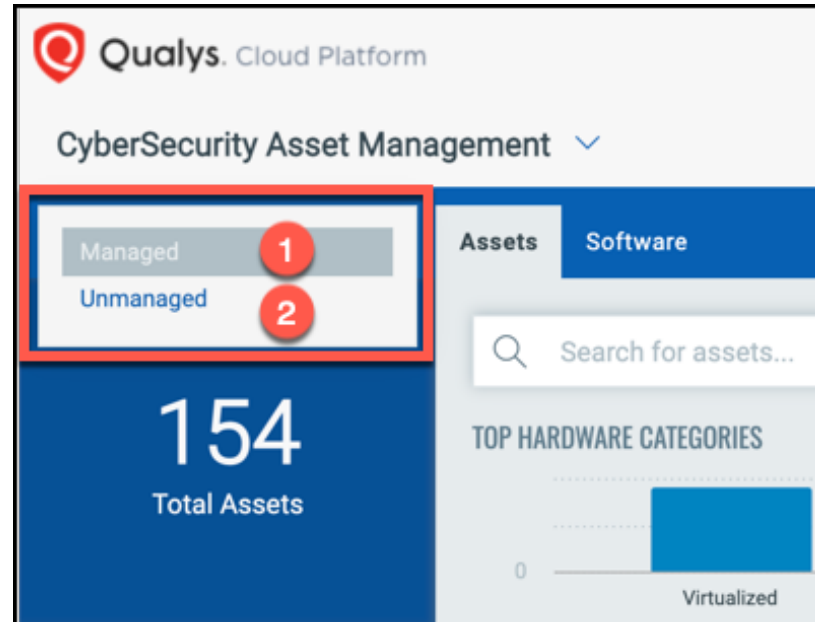


- Sniffs traffic via network TAP or the SPAN port of a network switch.
 - Captured data and traffic is sent to the Qualys Platform for analysis and processing.
1. Discovered assets not in your account, are placed in the “Unmanaged” section of Qualys CSAM.
 2. Enable “Traffic Analysis” to reveal communication between assets, including conversations between managed and unmanaged assets.

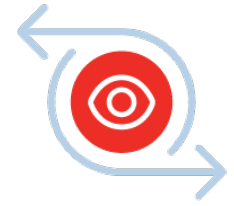
Managed vs. Unmanaged Assets



1. If discovered data is confirmed to match an asset already in your account, its information will be merged with the existing asset.
2. Discovered assets not in your account, are placed in the “Unmanaged” section of Qualys CSAM.



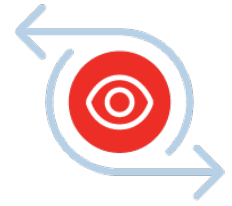
Unmanaged Assets



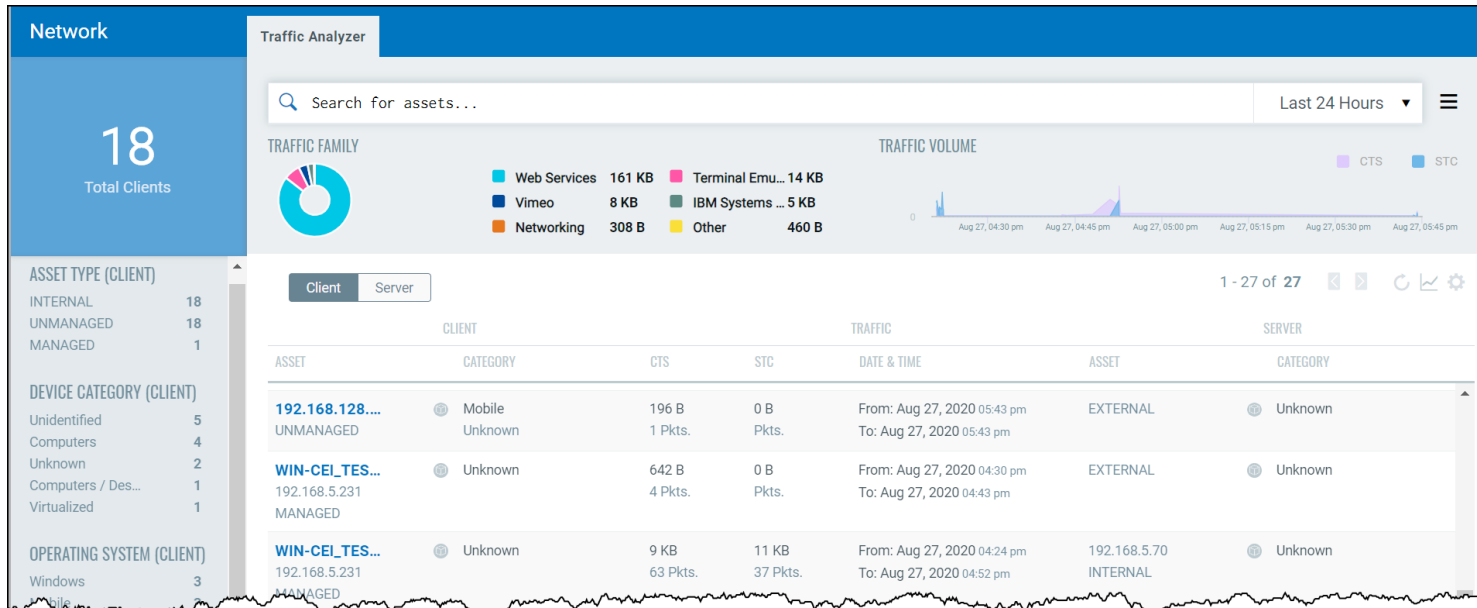
ASSET	OPERATING SYSTEM	HARDWARE	INVENTORY
- bc:a5:11:b8:e5:94	<div>▼ Confidence level: HIGH</div>	Series 24-... GS324TP S350 Series 24-...	Passive Sensor First: Sep 02 2020 Last: Sep 02 2020
Ubuntu19esxi 10.0.1.253 00:0c:29:82:ab:7a	Debian Project Debian	Unidentified	Passive Sensor First: Mar 26 2020 Last: Sep 02 2020
10.0.1.31			Passive Sensor

- It is common to find **unidentified** or **unknown** values within the "Unmanaged" assets section of the CyberSecurity Asset Management application.
- Confidence levels are provided (LOW, MEDIUM, HIGH) for OS and hardware findings.

Network Traffic Analyzer



- Conversations between assets can offer new discoveries and insights.



Network Passive Sensor User Guides



Qualys. Community

Discussions

Blog

Training

Docs

Support



Search documentation

qualys.com/documentation

Sensors

+ Cloud Agents

+ Scanner Appliance

— Network Passive Sensor

[Online Help](#)

[Getting Started Guide](#)

[Physical Appliance User Guide](#)

[Virtual Appliance User Guide](#)

[Deployment Guide](#)

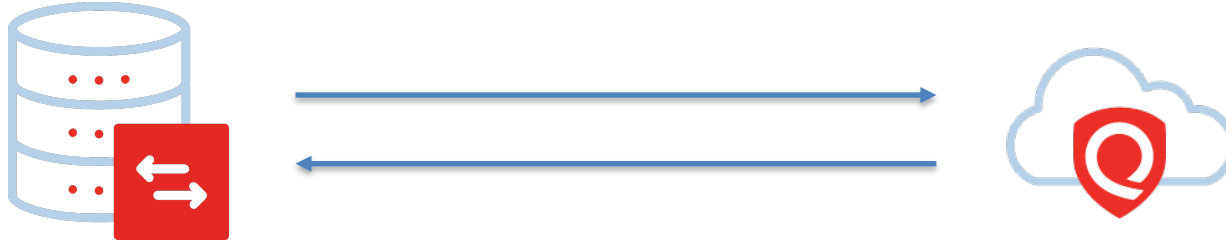
[Release Notes](#)

[Training](#)

✓ Stay up-to-date with the latest sensor features and specifications.

CMDB Sync

Certified ServiceNow CMDB Sync App



- Supports 2-way sync (Qualys to ServiceNow and ServiceNow to Qualys)
- Up-to-date, categorized, normalized, and enriched ServiceNow CMDB
- Enrich Qualys assets with key CMDB business data
- Synchronization schedules can be configured and saved.
- Asset metadata is only synchronized for assets that already exist in both Qualys and ServiceNow.
- Optionally, asset information is staged for user approval before being written to CMDB.

Import Business Attributes from ServiceNow CMDB

← Resource Details: 961701629973009803

Business Information

Status: Repair
Managed By: Byron Fortuna
Department: IT Operations
Supported By: John Doe

Business Applications

BUSINESS APP NAME	BUSINESS CRITICALITY	OPERATIONAL STATUS
Banking Service	1 - Most Critical	Installed

Business Application Details

Banking Service
Installed | Business Criticality: 1 - Most Critical

OVERVIEW **ASSOCIATED ASSETS**

1 - 4 of 4

ASSET	SYSTEM INFO	SUPPORTED BY
HQUIN8R2RD27 10.46.105.42,169.254.162.50,fe80...	Microsoft Windows Server 2008 R... VMware VMWare Virtual Platform ...	John Doe IT Operations
WIN12PMIOC3 10.0.1.6,169.254.5.79,192.168.13....	Microsoft Windows Server 2012 R... Google Compute Engine	John Doe IT Operations
10.115.75.59 10.115.75.59	The CentOS Project CentOS 7 (1511) VMware VMWare Virtual Platform ...	John Doe IT Operations

Close

- Automatically import business application and business context attributes from ServiceNow CMDB
- Identify other assets associated with a business application

Use Business Attributes to Search for Assets

businessApp:(businessCriticality

businessApp:(environment

businessApp:(id

businessApp:(managedBy

businessApp:(name

businessApp:(operationalStatus

businessApp:(ownedBy

businessApp:(supportGroup

businessApp:(supportedBy

- Use any of the “businessApp” search tokens to single out assets, based on the business information and characteristics provided by ServiceNow.
- Queries using these tokens will impact assets already synchronized.

Lab 4 : CMDB Sync and Business Context

Please consult pages 18 to 19 in the lab tutorial supplement for details.



Tutorial begins on page 18.

5 mins

Integration with ServiceNow CMDB

To implement ServiceNow CMDB Integration, a Qualys subscription with API access is required, along with the following application modules:

- CSAM
- Vulnerability Management

1. Qualys CMDB Sync App

- Install the Qualys CMDB Sync App (available in ServiceNow Online Store)

2. Qualys CMDB Sync Service Graph Connector App

- Install the Qualys Service Graph Connector App (available in ServiceNow Online Store)
- ITOM Visibility license in ServiceNow

CMDB Sync App User Guides



[Discussions](#) [Blog](#) [Training](#) **[Docs](#)** [Support](#)

 Search documentation

qualys.com/documentation

Cloud Apps

IT Asset Management

- + [Global AssetView](#)
- + [CyberSecurity Asset Management](#)
- + [AssetView](#)
- [CMDB Sync](#)
 - [Qualys CMDB Sync Service Graph Connector App](#)
 - [Qualys CMDB Sync App](#)
- + [Certificate Inventory](#)

Public APIs for CMDB Sync

- CSAM now supports import of **Asset business metadata** and **Business app metadata** from your CMDB into your Qualys asset inventory (using v2 APIs).
- Imported business attributes are listed in the Asset Details page.
- User must have access to the CSAM module with API enabled for that role.
- Currently supports maximum 250 records for import in one API call for both Asset and Business app metadata.

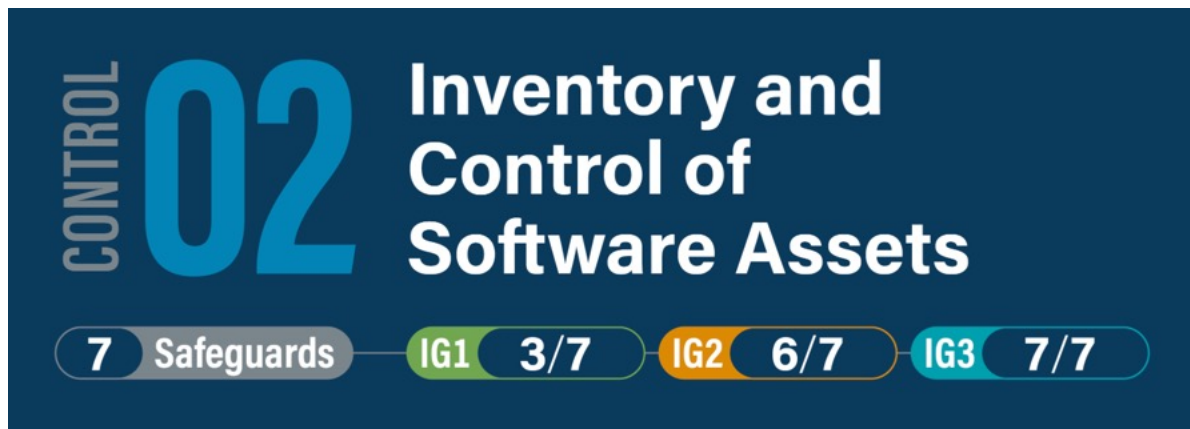
Authorized & Unauthorized Software

CIS Control 2: Inventory and Control of Software Assets



Overview

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.




<https://www.cisecurity.org/controls/inventory-and-control-of-software-assets/>

Software Rule Types


Select Software


Select the software to be included in the rule



Add Authorized Software 1


Select applications, releases, publishers or categories that are explicitly authorized in this environment.






Add Unauthorized Software 2


Select applications, releases, publishers or categories that are explicitly unauthorized in this environment.





Needs Review 3

Select applications, releases, publishers or categories that needs to be reviewed before marking as Authorized or Unauthorized.



- Create rules for authorized/unauthorized software and software that needs to be reviewed.

Lab 5: Software Authorization

Please consult pages 20 - 21 in the lab tutorial supplement for details.



Tutorial begins on page 20.

5 mins

Create Software Rules

Qualys. Cloud Platform

CyberSecurity Asset Management ▾ HOME DASHBOARD INVENTORY TAGS **RULES** RESPONSES

Software Rules

Actions (0) ▾ Reorder **Create Rule**

ORDER NUMBER	RULE
1	EOS Linux Agents Review all Linux agents less than
2	EOS Windows Agents Review Windows agent versions
3	Unauthorized Software Flag Wireshark as unauthorized

Assets **Software**

RELEASE	CATEGORY
Google Chrome 93.0.4577.82 Stable Channel	Network Application Internet Browser
Qualys Cloud Agent 4.4.1.7	Security Endpoint Management and Security
Microsoft Internet Information Services 94.0.992.3	Network Application Internet Browser
Apache Tomcat 9.0.52	Network Application Web Servers
Microsoft Internet Information Services 10.0	Network Application Web Servers
Qualys Cloud Agent 4.6.0.56	Security Endpoint Management and Security

- View, create and modify rules from the RULES section or the “Software” tab under the INVENTORY section.



Rule Precedence

Software Rules		
<input type="checkbox"/>	Actions (0) ▼	Reorder Create Rule Rules Software
ORDER NUMBER	RULE	STATUS
1	EOS Linux Agents Review all Linux agents less than version 2.6.	Enabled
2	EOS Windows Agents Review Windows agent versions less than 3.0.	Enabled
3	Unauthorized Software Flag Wireshark as unauthorized and Qualys Cloud Ag...	Enabled



- Rules at the top of the list have precedence over the rules below.
- Click the “Reorder” button to move rules higher or lower.

Software Authorization Tokens



- **AUTHORIZED**

 `software:(authorization:'Authorized')` 

- **UNAUTHORIZED**

 `software:(authorization:'Unauthorized')` 

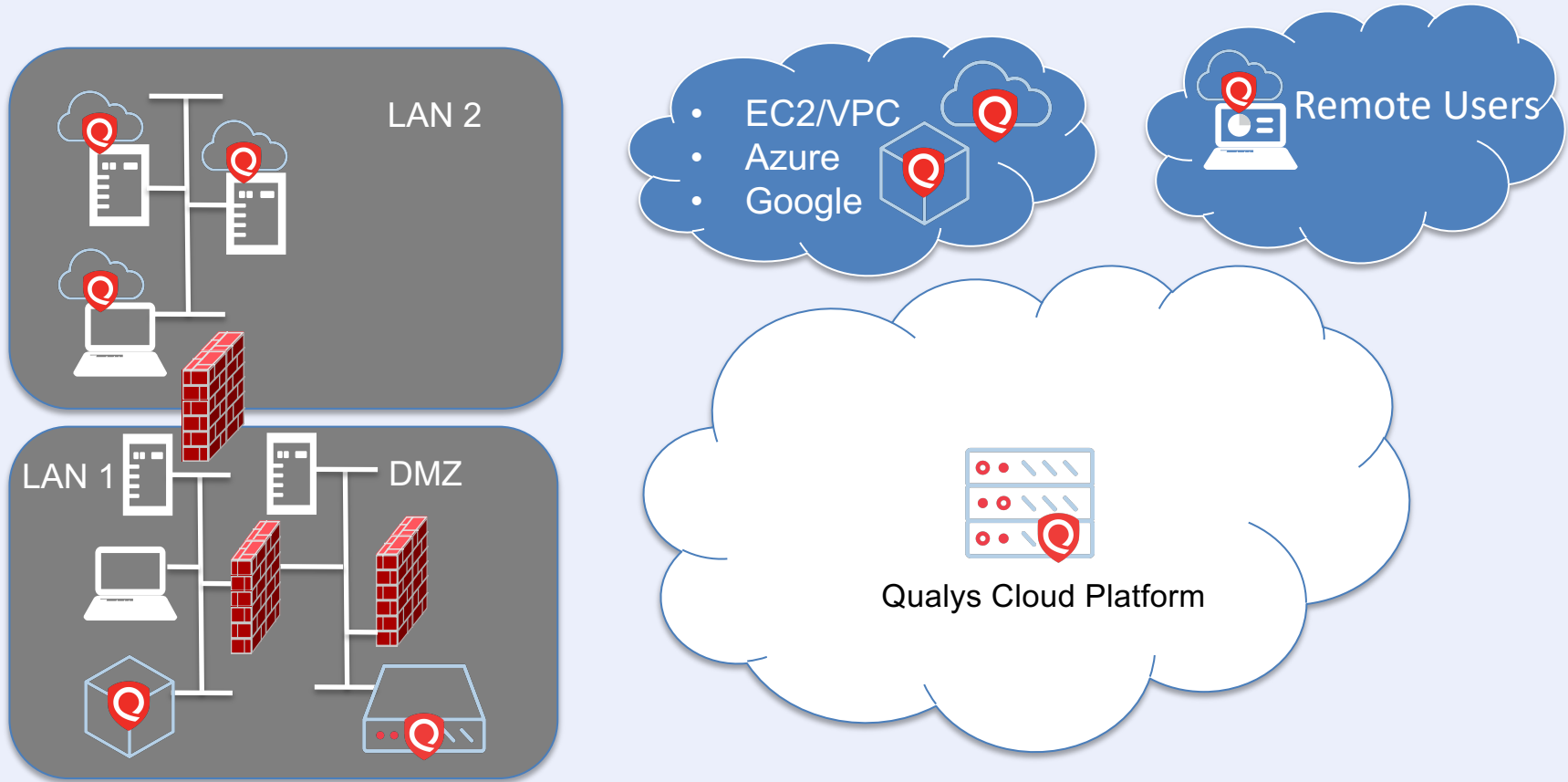
- **NEEDS REVIEW**

 `software:(authorization:'Needs Review')` 

- After creating software authorization rules, software authorization tokens can be used to search and query.




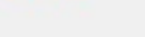

Vulnerability Management

VM Sensors



Vulnerability Findings

- Industry-leading vulnerability KnowledgeBase with tens-of-thousands of vulnerability signatures.
- Each vulnerability is ranked and associated with:
 - Qualys Severity Level
 - CVSS Score
 - CVE & Bugtraq IDs
 - Available Patches
 - Known Threats
 - Associated Malware
 - and more...
- An unlimited number of ways to identify, prioritize, and patch vulnerabilities.

Severity	Level
	Minimal
	Medium
	Serious
	Critical
	Urgent


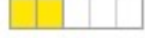
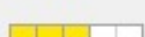
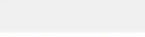
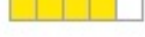
1

2

3

4

5

Severity	Level
	Minimal
	Medium
	Serious
	Critical
	Urgent

Lab 6 : Vulnerability Findings

Please consult pages 22 to 24 in the lab tutorial supplement for details.



Tutorial begins on page 23.

5 mins

Vulnerability Findings In CSAM

Asset Details: ws2016dfw242

INVENTORY

- Asset Summary
- System Information
- Network Information
- Open Ports
- Installed Software
- Traffic Summary

SECURITY

- Vulnerabilities**
- VMDR Prioritization
- Patch Management
- Certificates

Vulnerabilities

Search: vulnerabilities.severity:[5] and vulnerabilities.typeDetected:[Confirmed]

9 Vulnerabilities

1 - 9 of 9

QID	TITLE	SEVERITY	
91591	Microsoft Windows Security Update for December 2019 Active	■■■■■	Patch Now
91598	Microsoft .NET Framework Security Updates for January 2020 Active	■■■■■	Patch Now
100400	Microsoft Internet Explorer Remote Code Execution Vulnerability (AD... Active	■■■■■	Add to New Job Add to Existing Job View Missing Patches
100402	Microsoft Internet Explorer Security Update for March 2020 Active	■■■■■	
91609	Microsoft Windows Security Update for March 2020 Active	■■■■■	Patch Now
9746	Microsoft Windows Security Update for June 2020	■■■■■	Patch Now

Build Patch Jobs from Global IT Asset Inventory.

- View and patch vulnerability findings from within CyberSecurity Asset Management (on a per asset basis).

Vulnerability Findings in VMDR

Qualys Cloud Platform

VMDR TRIAL DASHBOARD **VULNERABILITIES** PRIORITIZATION SCANS REPORTS

Vulnerabilities

66
Total Detections

Vulnerability	Asset
<input type="checkbox"/> vulnerabilities.vulnerability.qualysPatchable:TRUE	<input type="checkbox"/> tags.name:'Cloud Agent' and activatedForModules:PM

☒ Actions (50) Group by ...

☒


ID	Description	Status
<input checked="" type="checkbox"/> 372508	Oracle Java SE Critical Patch Update - April 2020	Active
<input checked="" type="checkbox"/> 374827	Mozilla Firefox Multiple Vulnerabilities (MFS2021-01)	Active
<input checked="" type="checkbox"/> 374576	Mozilla Firefox Multiple Vulnerabilities (MFS2020-54)	Active

Which ones are patchable?

1. Detected vulnerabilities must be associated with one or more patches found in the Qualys Patch Catalog
2. Detection Host must be running the Qualys Cloud Agent
3. Cloud Agent must have the PM module activated

Dashboards & Widgets

Out-of-Box Dashboard Templates



← Dashboard Templates

Add or Customize Dashboard templates

OR

+ Build from Scratch

All (77)

CSAM (4)

Policy Compliance (1)

Unified Dashboard (35)

VMDR (16)


Web Application Firewall (1)

File Integrity Monitoring (6)

EDR (5)

Container Sec...

RansomWare (RW) Attack Ve...

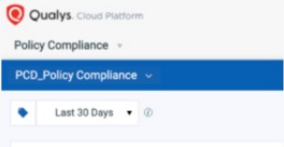


Ransomware Attack Vectors Dashboard provides high visibility into your Software and EOL/EOS...

Created By: Qualys

Use template

Policy Compliance




This dashboard provides Policy Compliance widget details.

Created By: Qualys

Use template

RansomWare (RW) Exposure




This Dashboard will enable any organization to have visibility into your RansomWare Exposure...

Created By: Qualys

Use template

Patch Efficiency - VULNs Sev...

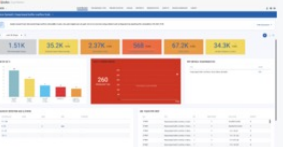


Patch Efficiency for vulnerabilities of Severity 3-5. This dashboard shows Patch Efficiency. It should...

Created By: Qualys

Use template

Baron Samedit|Heap-based b...




Qualys research team discovered heap overflow vulnerability in sudo. Any unprivileged user can...

Created By: Qualys

Use template

59

Qualys, Inc. Corporate Presentation



Widget Types



- Dashboard widgets can be designed to display query results as counts, tables, columns, or pie charts,

Lab 7 : Dashboards & Widgets

Please consult pages 25 to 28 in the lab tutorial supplement for details.



Tutorial begins on page 25.

5 mins

Count Widget

- The “Count Widget” can be configured to automatically change color, when specific conditions or thresholds are met.

The image shows the configuration interface for a 'Count Widget' on the left and its rendered output on the right. The configuration interface includes fields for the widget name, representation type (Regular/Summary), display results as (Asset/Vulnerability), count/ratio selection, two queries with filters, a comparison label, and a set of assets representation. The rendered output shows a red widget titled 'PERCENTAGE OF HIGH SEVERITY VULNERABILITIES' displaying '3.38K' vs 'All Vulnerabilities' (3.60K (94%)) with a '94.07%' change. The 'Widget Rules' section in the configuration interface is highlighted with a red box, showing a rule: 'When the value of the comparison percentage is greater than 50% highlight in' with a red color selection.

Configuration Interface:

- Name: Percentage of High Severity Vulnerabilities
- Widget Representation: Regular (selected), Summary
- Show description on widget: ☐
- Display results as: Asset, Vulnerability (selected)
- Count (selected), Ratio
- Query 1: Vulnerability, vulnerabilities.severity:[3,4,5]
- Compare with another reference query: ☒
- Query 2: Vulnerability, vulnerabilities.severity:[1,2,3,4,5]
- Comparison Label: All Vulnerabilities (i.e., all severities)
- This set of Assets represent: A superset (contains all the assets from initial query)

Rendered Output:

PERCENTAGE OF HIGH SEVERITY VULNERABILITIES

3.38K
vs All Vulnerabilities
3.60K (94%)
▼ 94.07%

Widget preferences
Choose a base color for the widget. This color will be displayed by default if no rules are set

Set Base Color: [Red]

When clicked navigate to: the targeted vulnerabilities search (grouped)

Widget Rules
Set rules and associated widget color. The widget color will be changed based on the condition satisfied for configured rules.

When the value of the comparison percentage is greater than 50% highlight in [Red]

+ Add another rule

Enable Trending in Widgets

The screenshot shows the 'Edit Widget (VM)' interface in the Qualys Cloud Platform. It features two query configuration sections and an 'Additional Options' section at the bottom. The 'Additional Options' section is highlighted with a red border and contains a checked checkbox for 'Enable Trending'. Below this checkbox, a text box explains that the widget will store results daily for up to 90 days for trend analysis. An inset window on the right displays a sample widget output: a large number '539' with a '139.56%' increase, a 'showing last 91 days' label with a gear icon, and a line graph showing a sharp drop in values over time.

Qualys Cloud Platform

← Edit Widget (VM)

Query 1

Vulnerability ☒ vulnerabilities.status:REOPENED

☒ Compare with another reference query

Query 2

Vulnerability ☒ vulnerabilities.status:[NEW,ACTIVE,REOPENED]

Additional Options

☒ Enable Trending

This widget will store its results each day for up to 90 days. The results will be plotted on a graph so that the data may be analyzed to identify trends.

2021

539

↑ 139.56%

showing last 91 days

0 7/13 Today

- Visualize changes or swings in momentum or progress.
- When enabled, widgets can store trend data for up to 90 days.
- Trend lines plotted on a graph are added to the widget.

Dashboard Tags

Edit Dashboard

User Edit: Bob Slydell (quays2bs38) Turn help tips: On | Off

Edit Mode

- User Details
- Profile Settings
- Roles And Scopes**
- Action Log
- Account Activity

Edit role(s) and scope

☐ **Allow user full permissions and scope** (The user will have full access to everything)

Each role grants you a set of permissions that will apply to the objects you have access to.

New role Search unassigned roles

Assigned roles	Remove all
AUDITOR	Remove
CA API Access	Remove
CA MANAGER	Remove
CA UI Access	Remove
CM User	Remove

Unassigned roles	Add all
ADMINISTRATOR	Add
CLOUDVIEW User	Add
CONTACT	Add
CSAM Manager	Add
CSAM User	Add

Edit Scope

☐ **Allow user view access to all objects** (Other permissions are granted by the user's roles)

Define what assets the user can access by tags.

Global Scope Select | Create | Remove All

Default Dashboard... X

☐ Exclude Agent assets from IP Range Tags

- Add one or more Asset Tags through the Dashboard Editor.
- The “Default Dashboard Access Tag” is created by Qualys.

Default Dashboard Access Tag

- Share dashboards with other Qualys users by assigning “dashboard” tag(s) to their accounts.

Session Break

30 min.



Threat Detection & Prioritization

VMDR Threat Feed

The screenshot shows the Qualys Cloud Platform VMDR interface. The top navigation bar includes 'DASHBOARD', 'VULNERABILITIES', 'PRIORITIZATION' (selected), 'KNOWLEDGEBASE', and 'USER'. The 'PRIORITIZATION' section has sub-tabs for 'Prioritization', 'Reports', and 'Threat Feed' (selected). A search bar at the top of the Threat Feed contains the text 'contents: RDP'. Below the search bar is a filter for 'Impacted Assets'. The main content area displays three threat feeds: 'HIGH RATED FEED' (429 items), 'MEDIUM / LOW RATED FEED' (59 items), and 'FAVORITES' (5 items). The 'HIGH RATED FEED' shows two threats: 'Microsoft Windows security update for October 2021...' (High severity, 2 days ago, 6 impacted assets) and 'Apple releases emergency update to address the arbitrar...' (High severity, 3 days ago, 0 impacted assets). The 'MEDIUM / LOW RATED FEED' shows one threat: 'Backdoor Account in Zyxel Products (CVE-2020-29583)' (Low severity, January 3, 2021, 0 impacted assets). The 'FAVORITES' section shows one threat: 'Microsoft Windows N...' (High severity, 0 impacted assets). Annotations include a red box around the search bar with the text 'Search for threats by category, content, or publish date.' and a red box around the '6 Impacted Assets' link with the text 'Click to view impacted assets within your subscription'.

Qualys Cloud Platform

VMDR

DASHBOARD VULNERABILITIES PRIORITIZATION KNOWLEDGEBASE USER

Prioritization Reports Threat Feed

Search: contents: RDP

Impacted Assets

HIGH RATED FEED 429

High 2 days ago 07:00 pm ☆ ≡

Microsoft Windows security update for October 2021...

Live Threat Intelligence Feed Microsoft October 2021 patch Tuesday has arrived with the latest updates! In this month's security update, Microsoft has fixed a total of 74 flaws including four zero-day vulnerabilities. Out o...

6 Impacted Assets

Low January 3, 2021 ☆ ≡

Backdoor Account in Zyxel Products (CVE-2020-29583)

Live Threat Intelligence Feed On December 23rd, 2020, Zyxel published an advisory for a hardcoded credential vulnerability. More than 100,000 Zyxel firewalls, access point controllers and VPN gateways are prone to this...

0 Impacted Assets

High ☆ ≡

Microsoft Windows N

Live Threat Intelligence Fe zero-day remote code exe component of the Internet

High ☆ ≡

Most Exploited Vulne

Live Threat Intelligence Fe Infrastructure Security Ag Security Centre (ACSC), th

3 days ago 07:00 pm ☆ ≡

Apple releases emergency update to address the arbitrar...

Live Threat Intelligence Feed On Monday, Apple released an iPhone security update to fix a major vulnerability that is being exploited in the wild. With the latest patch, the corporation has now resolved a total of 1...

0 Impacted Assets

Click to view impacted assets within your subscription

- Search for threats by content, category or publish date and click to view impacted assets.

Threat Feed Sources

Exploit Sources

Source Type	Data Type
Core Security	PoC Exploits mapped to CVEs
Exploit-DB	PoC Exploits mapped to CVEs
Metasploit	PoC Exploits mapped to CVEs
Contagio Dump	Exploit Kits mapped to CVEs
Immunity - Agora - Dsquare - Enable Security - White Phosphorus	PoC Exploits mapped to CVEs
Google Project Zero	Zero-Days mapped to CVEs

Malware Sources

Source Type	Data Type
Reversing Labs	CVEs associated with malware
Trend Micro	Malware names associated with CVEs
McAfee	Ransomware mapped to CVEs

- The Qualys Threat and Malware research team leverages exploit and malware data from multiple sources.

VMDR Prioritization Report



Welcome to VMDR Prioritization

Prioritize your remediation activities by adding threat intelligence and asset context to your vulnerabilities



Prioritize vulnerabilities by:

- Asset Context
- Vulnerability Age
- Threat Intelligence
- Attack Surface

Lab 8: VMDR Prioritization Report

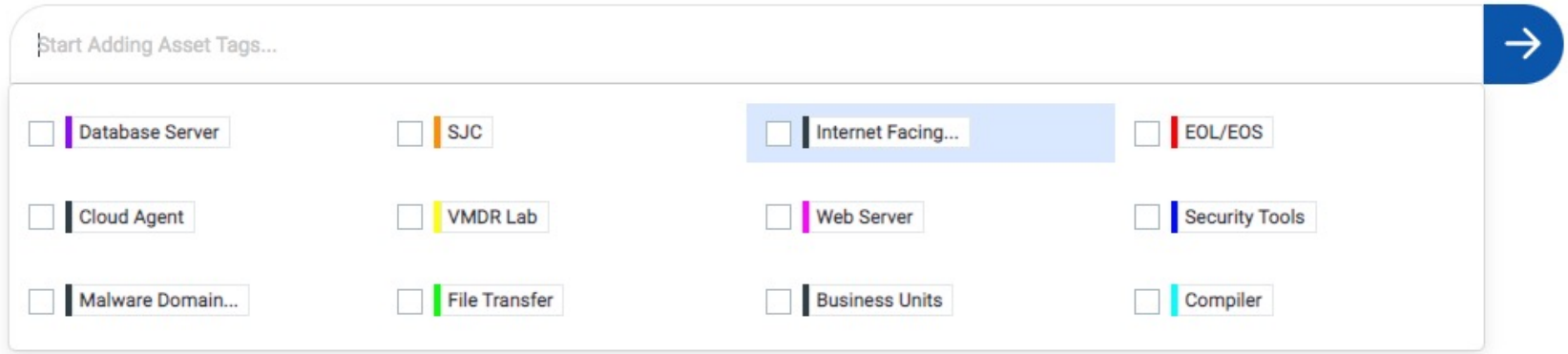
Please consult pages 29 to 35 in the lab tutorial supplement for details.



Tutorial begins on page 30.

5 min.

Asset Tags Add Context

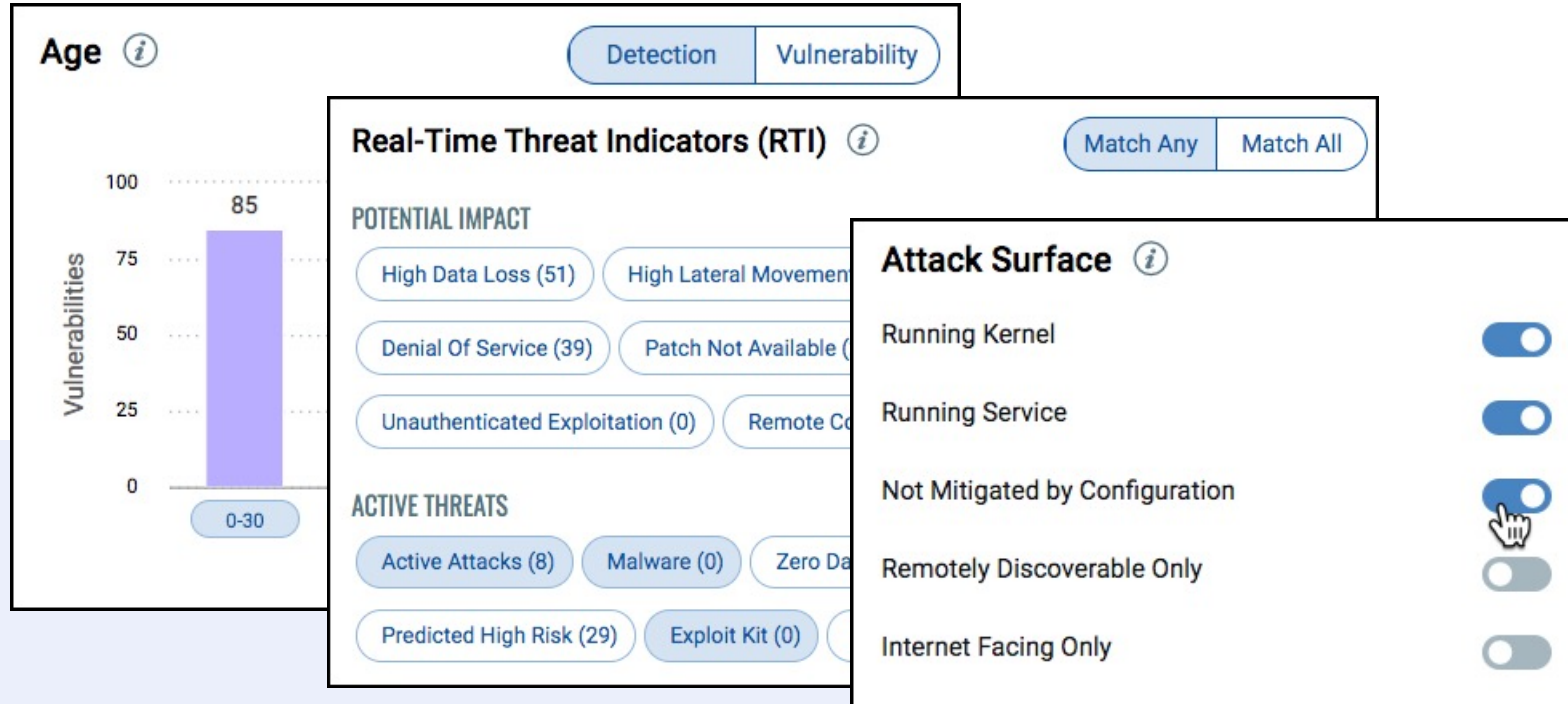


The screenshot shows a user interface for adding asset tags. At the top, there is a header bar with the text "Start Adding Asset Tags..." and a blue button with a white right-pointing arrow. Below the header, there is a grid of 12 asset tags, each consisting of a checkbox and a label. The tags are arranged in three rows and four columns. The "Internet Facing..." tag in the first row, third column is highlighted with a light blue background.

Database Server	SJC	Internet Facing...	EOL/EOS
Cloud Agent	VMDR Lab	Web Server	Security Tools
Malware Domain...	File Transfer	Business Units	Compiler

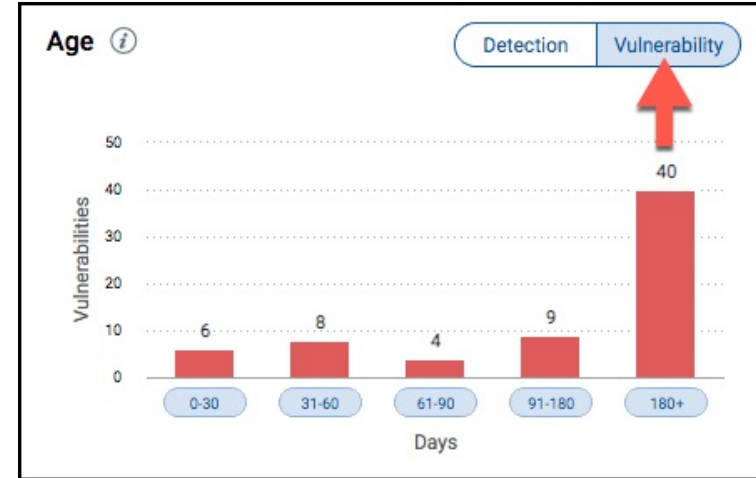
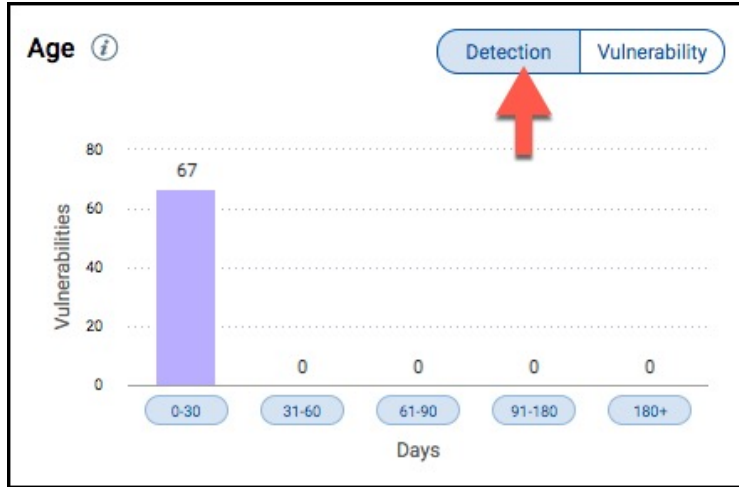
- Design and build Asset Tags that help to distinguish the “context” of your assets.
- Leverage tags that use the “Asset Inventory” rule engine, along with 1) **hardware**, 2) **software**, and 3) **OS** categories.

Priority Options



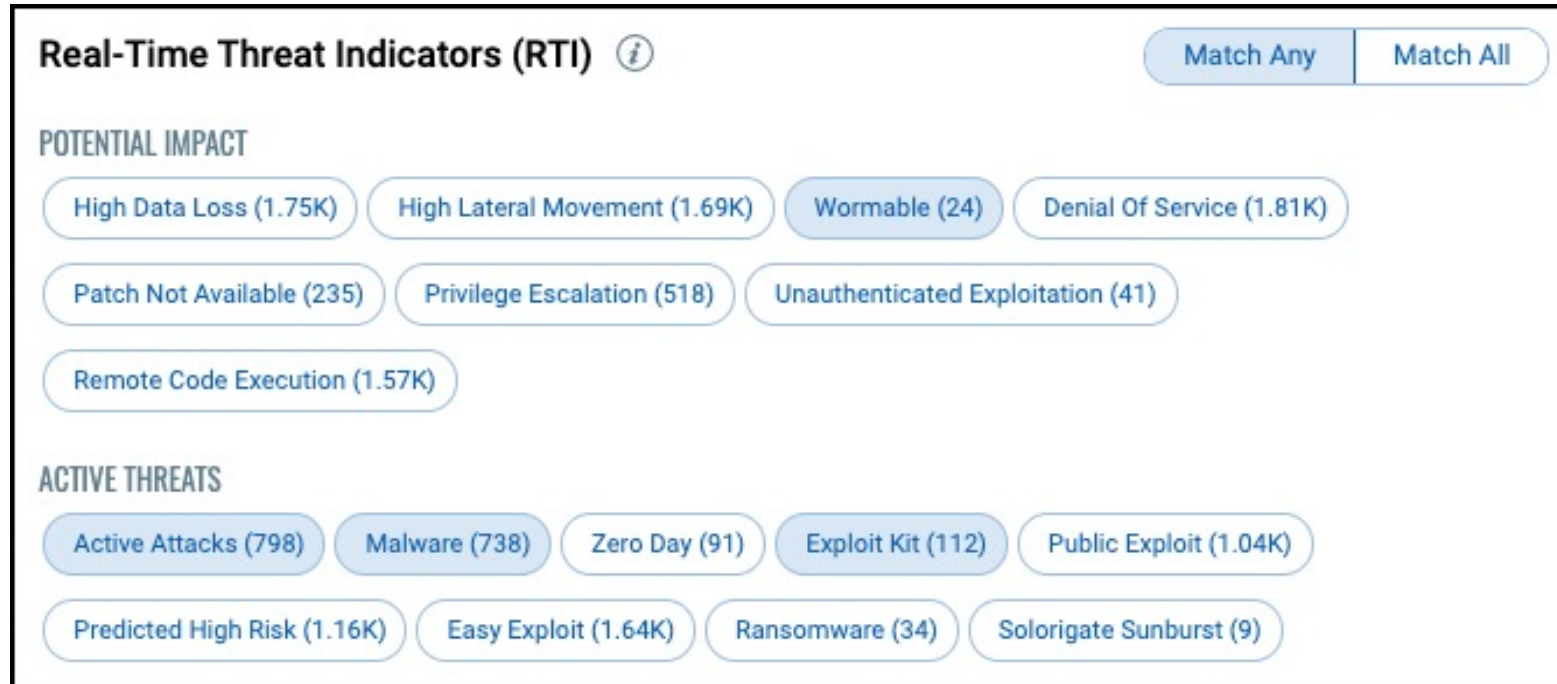
- Prioritize discovered vulnerabilities by Age, RTIs, and Attack Surface.

Age



- **Detection Age** – reflects the number of days since you first detected the vulnerability (e.g., by Qualys scanner or Cloud Agent).
- **Vulnerability Age** – (i.e., real age) reflects the number days since Qualys published the vulnerability to our KnowledgeBase.

Real-Time Threat Indicators (RTI)



- Provided by VMDR Threat Feed.

Attack Surface

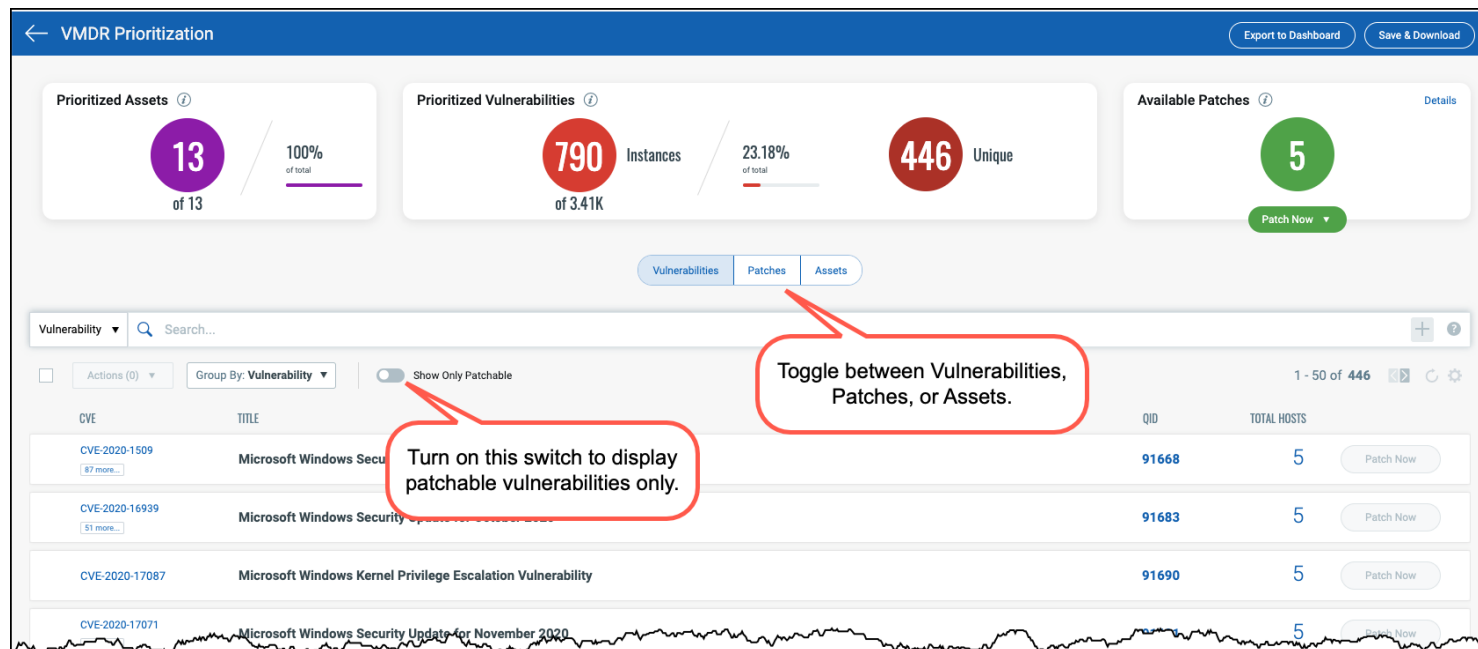
Attack Surface ⓘ

Running Kernel	<input checked="" type="checkbox"/>
Running Service	<input checked="" type="checkbox"/>
Not Mitigated by Configuration	<input checked="" type="checkbox"/>
Remotely Discoverable Only	<input type="checkbox"/>
Internet Facing Only	<input type="checkbox"/>

- Continue to define asset context with “Attack Surface” options.

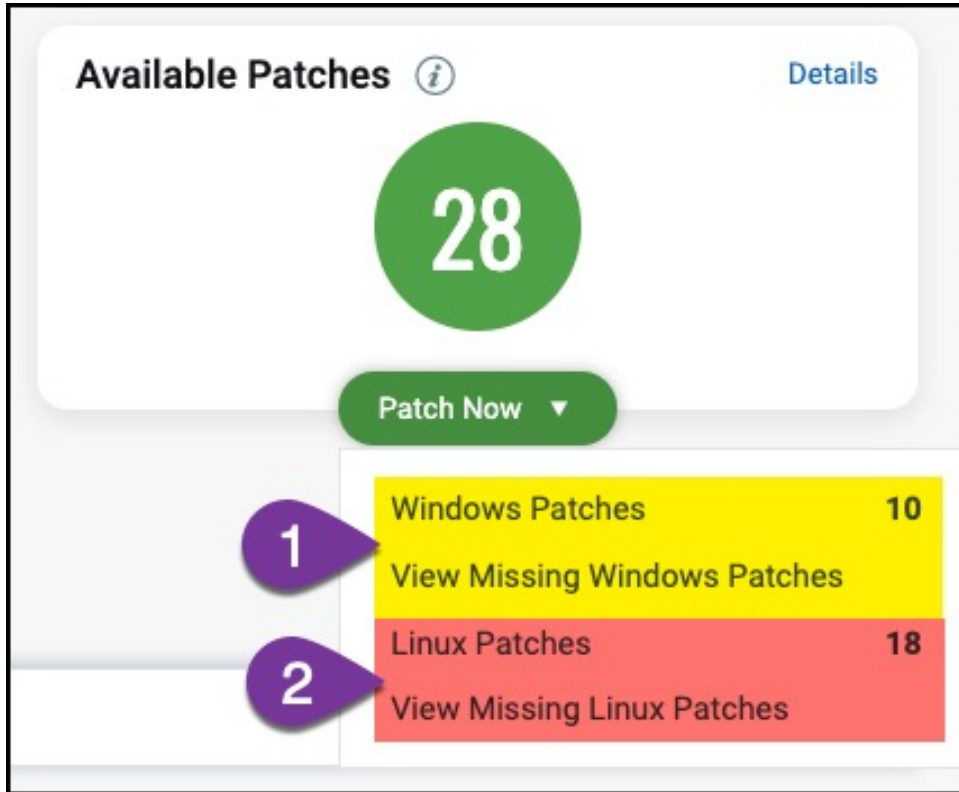
Deploy Priority Patches

Prioritize Now



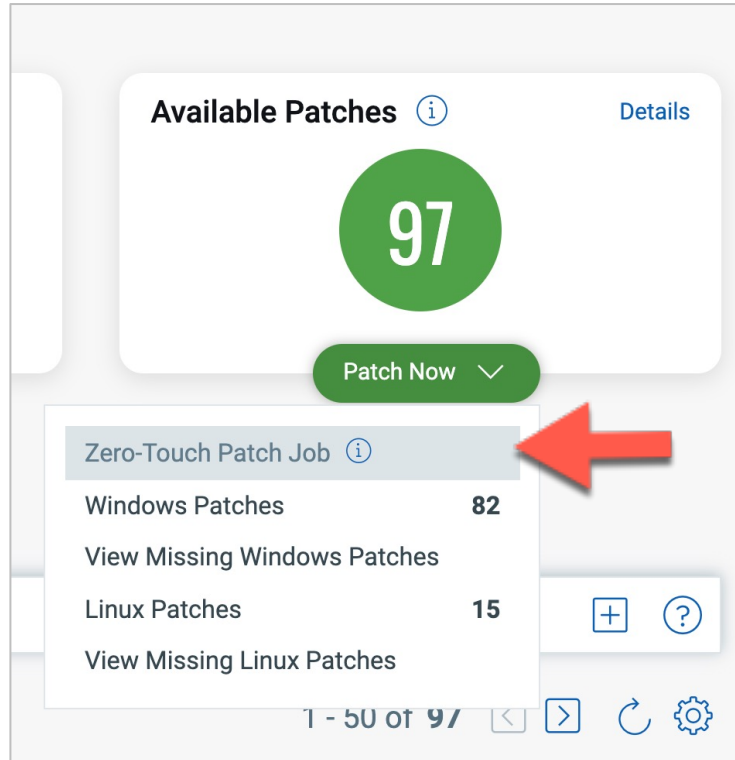
- Patchable assets have Cloud Agent installed and Patch Management activated.

Windows & Linux Patches



1. Available patches provided for Windows hosts.
2. Available patches provide for Linux hosts.

Zero-Touch Patch Job



- Select the “Zero-Touch Patch Job” option from the VMDR Prioritization Report.
- Patches are not selected individually, but instead are targeted using a query.
- Schedule patch jobs to recur daily, weekly, or monthly.
- Specific patching use-cases are ideal for “Zero-Touch” patching.

Zero-Touch Patching

Create: Windows Deployment Job

STEPS 4/9

- 1 Basic Information
- 2 Select Assets
- 3 Select Pre-actions
- 4 **Select Patches**
- 5 Select Post-actions
- 6 Schedule
- 7 Options

Select Patches

Choose the patches you want to install for the selected assets or create a query to automate the job.

☐ Manual Patch Selection
Select manually from the available list of patches.

☒ Automated Patch Selection
Define QQL to automatically identify patches to remediate current and future vulnerabilities every time the job runs.

Vulnerability

X

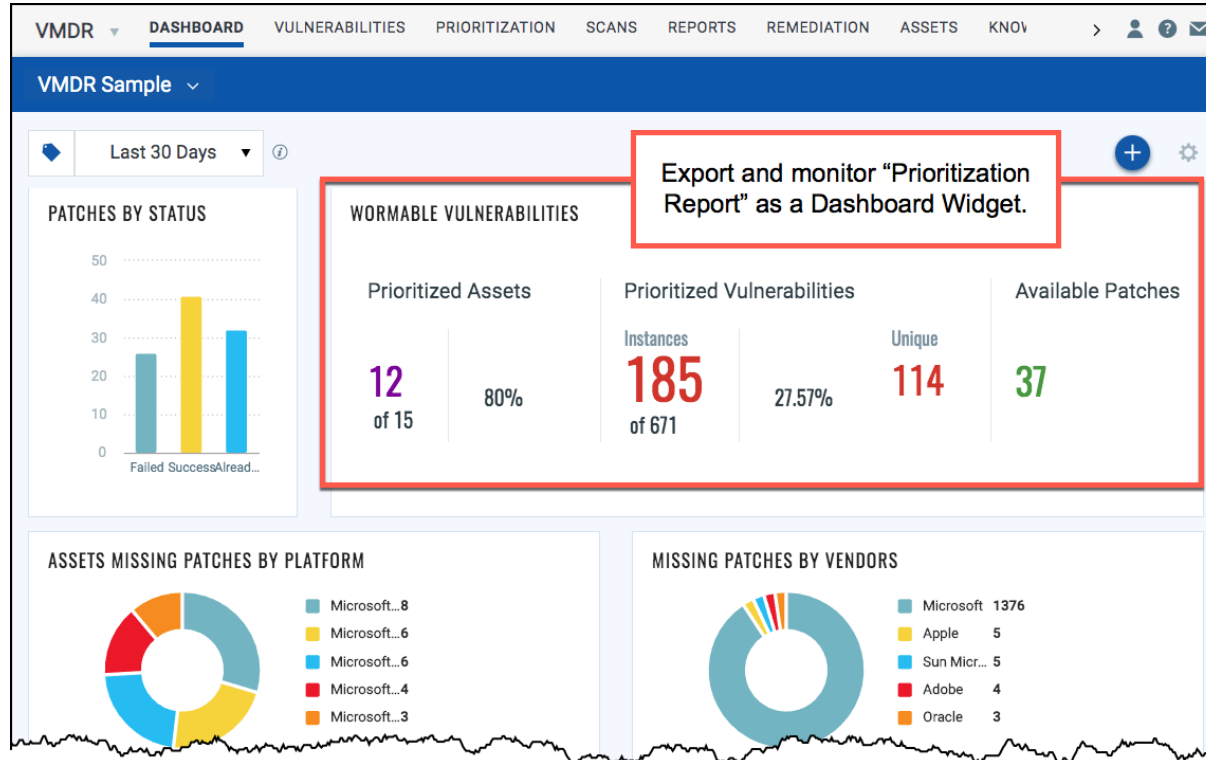
`(vulnerabilities.vulnerability:(threatIntel.malware:True or threatIntel.activeAttacks:`

Note: For optimum performance, only missing and non-superseded patches that match the QQL criteria will be added to the job.

Patches that meet the query condition are added to the deployment job, automatically.

- The query is generated from the options (Age, RTIs, and Attack Surface) selected in the Prioritization Report.

Export to Dashboard



Results will be continuously updated within the Dashboard Widget.

Labs 9 & 10 : Prioritization Report Use-Cases

Please consult page 36 in the lab tutorial supplement for details.



Tutorials begins on page 36.

10 mins

Patch Management

Patch Management Features & Benefits

- Automatically correlates discovered vulnerabilities with their required patches.
- Leverage existing Qualys Agents to deploy and uninstall patches.
- Covers OS and Application patches, including patches from third-party software vendors (e.g., Adobe, Java, Google, Mozilla, Microsoft, etc...)
- Provides patching just about anywhere an Internet connection is available (e.g., airports, coffee shops, remote offices, etc...).
- Focus on missing patches that have not been superseded.
- Build patch jobs that target specific vulnerabilities, severity levels, and known threats.

Patch Sources

OS and Application Patches come from:

- Vendor Global CDNs (e.g., Oracle, Adobe, Microsoft, Apache, Google, etc...)
 - Qualys uses both digital signatures and hash values to validate downloaded patches, which are validated again, via Qualys Malware Insights.
- Local repository (i.e., Qualys Gateway Server)
 - Patch downloads requested by one agent, are cached on QGS and made available “locally” for other agents that need the same patch.

Qualys PM Workflow

CA

1. Install Cloud Agent on target host.

CA

2. Assign target agent host to a CA Configuration Profile that has PM configuration enabled.

CA

3. Activate PM module on target agent host.

PM

4. Assign target agent host to an enabled Assessment Profile.

PM

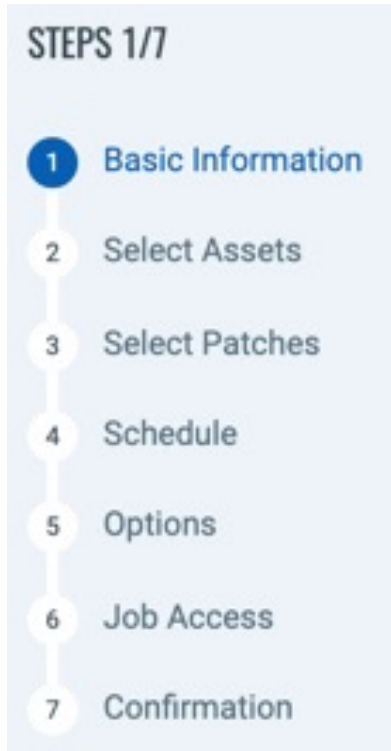
5. Allocate patching licenses.

PM

6. Create Patch Jobs.

Patch Deployment Job

Deployment Job Wizard



- Build patch jobs step-by-step.
- Select assets and patches.
- Configure scheduling option or run on-demand.
- Configure communication and reboot options.
- Assign access to a job.

Lab 11 : Patch Deployment

Please consult pages 37 to 41 in the lab tutorial supplement for details.




Tutorial begins on page 37

10 mins

License Consumption

License Consumption



Patch Management

Type: **FULL**
Expiring in: **3.04K days** on **Jan 31, 2030 05:59 pm** Status: **ACTIVE**

Total Consumption

9 Of 100

100%

Select assets for patch management

Select asset tags to include or exclude for patch management. Total Consumption counter shows the number of licenses used based on the number of matching assets contained in the included asset tags.

Include Assets Tags

Cloud Agent X

☒ Add Exclusion Asset Tags

Exclude Assets Tags

Don't Patch X

Exclude assets you do not want to patch.

Select Tags

- Use Asset Tags to specify hosts for patching and to exclude others.
- Only agent host assets will consume a patch license.

Targeted Assets

Select Assets

Select the assets you want this job to deploy patches on.

Include the following assets.

Selected Assets (1)

ASSET NAME

WS2019-VL50D6A

Add Assets

Remove All

☐ Add Exclusion Assets

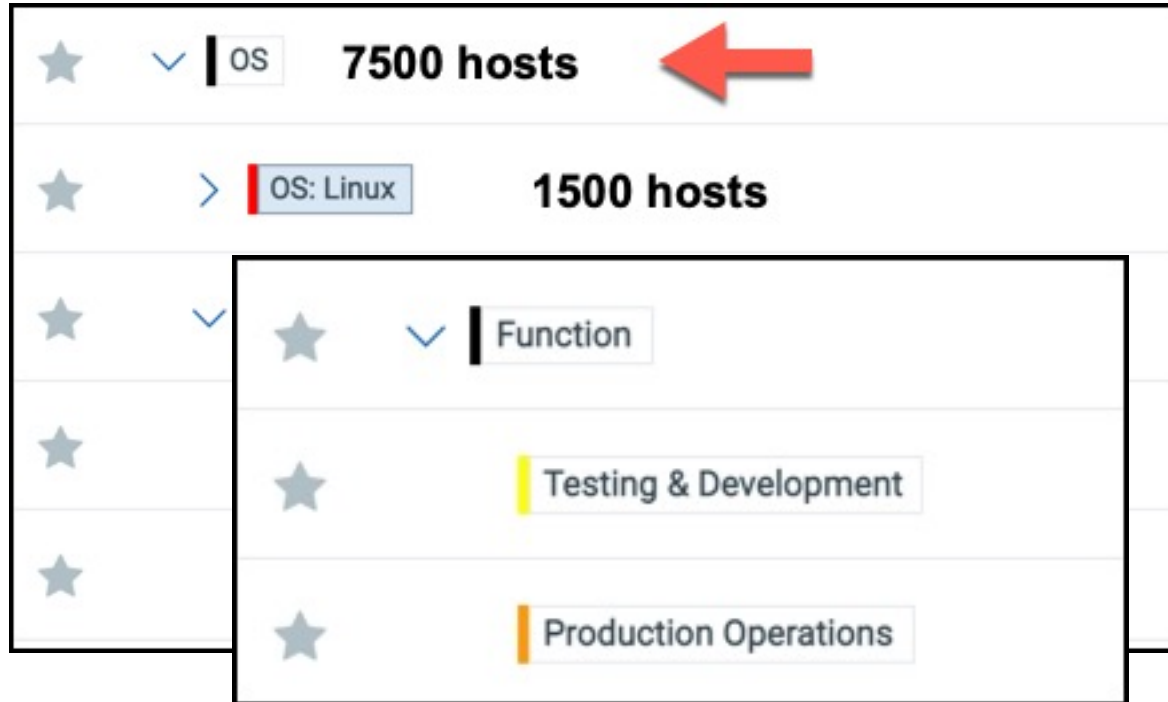
Include hosts that have Any ▼ of the tags below.

OS: Windows Server

Select Tags

- Add assets to a Deployment Job by Asset Name or Asset Tag.
- Asset Tags are automatically transferred from VMDR Prioritization Report.

Asset Tag Tips



- Design Asset Tag hierarchies with nested structures.
- Selecting a “parent” tag as a patching target, includes its “child” tags automatically.
- Use tags to distinguish between production and testing assets.

Targeted Patches

The screenshot shows the 'Patch Selector' interface. On the left, a sidebar indicates '31 Total Patches' and lists categories: 'SUPERSEDED' (false, 31) and 'APP FAMILY' (Windows: 26, .Net: 2, Tomcat: 1, Firefox: 1, Java: 1). The main area features a search bar with the filter 'isSuperseded:false' (highlighted by a red arrow), a 'Within Scope' filter, and an 'Add to Job (31)' button. Below this is a table of patches with columns: PATCH TITLE, ARCHIT, BULLETIN, QID, VENDOR SEVERITY, and CVE. The table lists five patches, including 'Cumulative Update f...', 'July 21, 2020-KB45...', 'July 14, 2020-KB45...', 'Security Cumulative...', and 'Servicing stack up...'. The 'VENDOR SEVERITY' column shows 'None' for the first two and 'Critical' for the last three. The 'CVE' column shows 'CVE-2020-1390' for the last two and 'CVE-2020-1346' for the last one.

PATCH TITLE	ARCHIT	BULLETIN	QID	VENDOR SEVERITY	CVE
<input checked="" type="checkbox"/> Cumulative Update f... Published on Jul 20, 2020	⏻ X64	MSNS20-07-W...	91495 97 more...	None	—
<input checked="" type="checkbox"/> July 21, 2020-KB45... Published on Jul 20, 2020	⏻ X64	MSNS20-07-M...	91552 14 more...	None	—
<input checked="" type="checkbox"/> July 14, 2020-KB45... Published on Jul 14, 2020	⏻ X64	MS20-07-SO81...	91662 2 more...	Critical	CVE-2020-1390 40 more...
<input checked="" type="checkbox"/> Security Cumulative... Published on Jul 13, 2020	⏻ X64	MS20-07-W10...	91410 225 more...	Critical	CVE-2020-1390 67 more...
<input checked="" type="checkbox"/> Servicing stack up...	⏻ X64	MS20-07-SSU...	91653	Critical	CVE-2020-1346

- Build more efficient patch jobs by focusing on patches that have not been superseded.

Select Patches Using QQL

Qualys Cloud Platform

← Create: Windows Deployment Job

STEPS 3/7

- 1 Basic Information
- 2 Select Assets
- 3 Select Patches
- 4 Schedule
- 5 Options
- 6 Job Access
- 7 Confirmation

Select Patches

Choose the patches you want to install for the selected assets or create a query for the job.

☐ Select Patches ☒ Create a Query for Patches

Patch

Patch
Vulnerability

Query by Patch or Vulnerability

Cancel Previous Next

- The query specifies the targeted patches.
- Choose between Patch or Vulnerability when constructing a query.

“Within Scope” Patch



- “Within Scope” only includes patches needed by your targeted host assets.

Schedule Deployment

Schedule Deployment

Schedule the deployment job to run on demand or in the future.

On Demand

Schedule

Schedule: Schedule the deployment job to run at a set time.

START DATE

09/01/2027

START TIME

12:30am

REPEATS

Daily

Daily

Weekly

Monthly

TIMEZONE

By default the system will use the agent timezone. [Set timezone](#)

Patch Window

You can configure a patch window to run the deployment job only during the specified time frame.

☒ None

☐ Set Duration

Note: Not setting the patch window will allow the cloud agent to take as much time as it needs to complete the job.

- Run jobs "on demand" or schedule them to run at regular frequencies.

Patch Window

Patch Window

You can configure a patch window to run the deployment job only within a particular time frame.

☐ None ☒ Set Duration 

Note: Setting this will restrict the agent to complete the job within the specified patch window (e.g., start time + 6 hrs). The job gets timed out outside this window.

Patch Window

- A host will display the “Timed out” status, if the patch installation does not **start** within a specified patch window.
- Select the “None” option to give agents an unlimited amount of time.

Windows Communication Options

Deployment and Reboot Communication Options

Define user (recipient) patch deployment communication and reboot warning messages to encourage and educate the user about patch installment and the reboot cycle.

Reboot messages

Suppress Reboot
Asset reboot is suppressed and users are not prompted for reboot post patch installation.

☐ OFF

Reboot Request
Show a message to users indicating that a reboot is required.
(If no user is logged in, the reboot will start immediately after patch deployment)

☐ OFF

Reboot Countdown
Show countdown message to users after deferment limit is reached.

☐ OFF

- Choose the type of “Deployment and Reboot Communication Options” for each Deployment Job.

Opportunistic Patch Download

Additional Job Settings

Enable opportunistic patch download
The agent attempts to download patches before a scheduled job runs.

ON ☒

Minimize job progress window
Allow end-users to minimize message windows.

☐ OFF

- You can “Enable opportunistic patch download,” to allow agents to download required patches prior to the start of a **scheduled** job.

Linux Communication Options

Reboot Communication Options

Define user (recipient) patch deployment communication and reboot warning messages to encourage and educate the user about patch installment and the reboot cycle.

Reboot messages

Suppress Reboot

Asset reboot is suppressed and users are not prompted for reboot post patch installation.

☐ OFF

Reboot Countdown

Show countdown message to users after deferment limit is reached.

☐ OFF

- Suppress Reboot and Reboot Countdown

Add to Existing Job?

← Add Patches: Existing Deployment Jobs			
STATUS	JOB NAME	CREATED BY	SCHEDULE
✓ Enabled	Scheduled - Recurring Created by trann3zd54 on Jul 3...	trann3zd54 Jul 30, 2020	Every 30th day of the ...
✓ Disabled	Scheduled - Run Once Created by trann3zd54 on Jul 3...	trann3zd54 Jul 30, 2020	Once, Aug 30 2020 7:...
✓ Disabled	On Demand - Run Now Created by trann3zd54 on Jul 3...	trann3zd54 Jul 30, 2020	On-demand

- Patches and assets can be added to any deployment job, before it is enabled
- Patches and assets can be added to a “recurring” job, both before and after it is enabled.

Best Practices

- Use Asset Tags as targets for patch deployment jobs.
- Deploy patches to test hosts, first (create Asset Tags that distinguish between test and production assets).
- Once test deployments are verified, **clone the deployment job** and include production asset tags

Patch Catalog

Patches

The screenshot displays the 'Patch Management' dashboard. The top navigation bar includes 'DASHBOARD', 'PATCHES' (selected), 'ASSETS', 'JOBS', and 'CONFIGURATION'. The 'Patch Catalog' section shows a total of 35.3K patches. On the left, there are filters for 'APP FAMILY' (Windows: 17.8K, Office: 4.18K, Internet Explorer: 2.93K, Office Viewer: 1.41K, Lync: 1.17K, 45 more) and 'VENDOR' (Microsoft: 27.8K, Mozilla Foundati...: 870, Adobe: 657, Google: 596, Opera Software A...: 420, 45 more). The main table lists patches with columns: PATCH TITLE, ARCHIT, BULLETIN / KB, TYPE, QID, VENDOR SEVERITY, and PATCH STATUS (MISSING, INSTALLED). The table shows several entries, including 'Snagit 2019.1.7' and 'August 4, 2020, updat...' with various severity levels (Moderate, Critical) and counts of missing and installed patches.

PATCH TITLE	ARCHIT	BULLETIN / KB	TYPE	QID	VENDOR SEVERITY	PATCH STATUS	
						MISSING	INSTALLED
Snagit 2019.1.7 Published on Aug 03, 2020	X86	SNAG19-200804 QSNAG1917	Application	372059	Moderate	0	0
Snagit 2018.2.6 Published on Aug 03, 2020	X86	SNAG18-200804 QSNAG1826	Application	372059	Moderate	0	0
August 4, 2020, updat... Published on Aug 03, 2020	X86	MSNS20-08-4484477 KB4484477	Application	—	Critical	0	0
August 4, 2020, updat... Published on Aug 03, 2020	X86	MSNS20-08-4484464 KB4484464	Application	—	Critical	0	0
Snagit 2019.1.7 Published on Aug 03, 2020	X86	SNAG19-200804 QSNAG1917	Application	372059	Moderate	0	0
Snagit 2019.1.7 Published on Aug 03, 2020	X86	SNAG19-200804 QSNAG1917	Application	372059	Moderate	0	0

- The Patch Catalog contains tens of thousands of OS and application patches.
- Presently, you can add up to 2000 patches to a single job.

Lab 12 : Patch Catalog

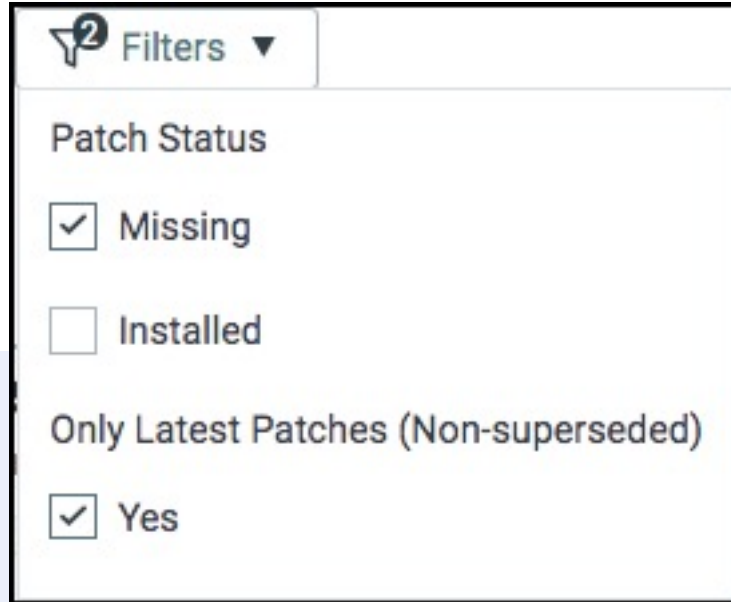
Please consult pages 42 to 46 in the lab tutorial supplement for details.



Tutorial begins on page 42.

10 mins

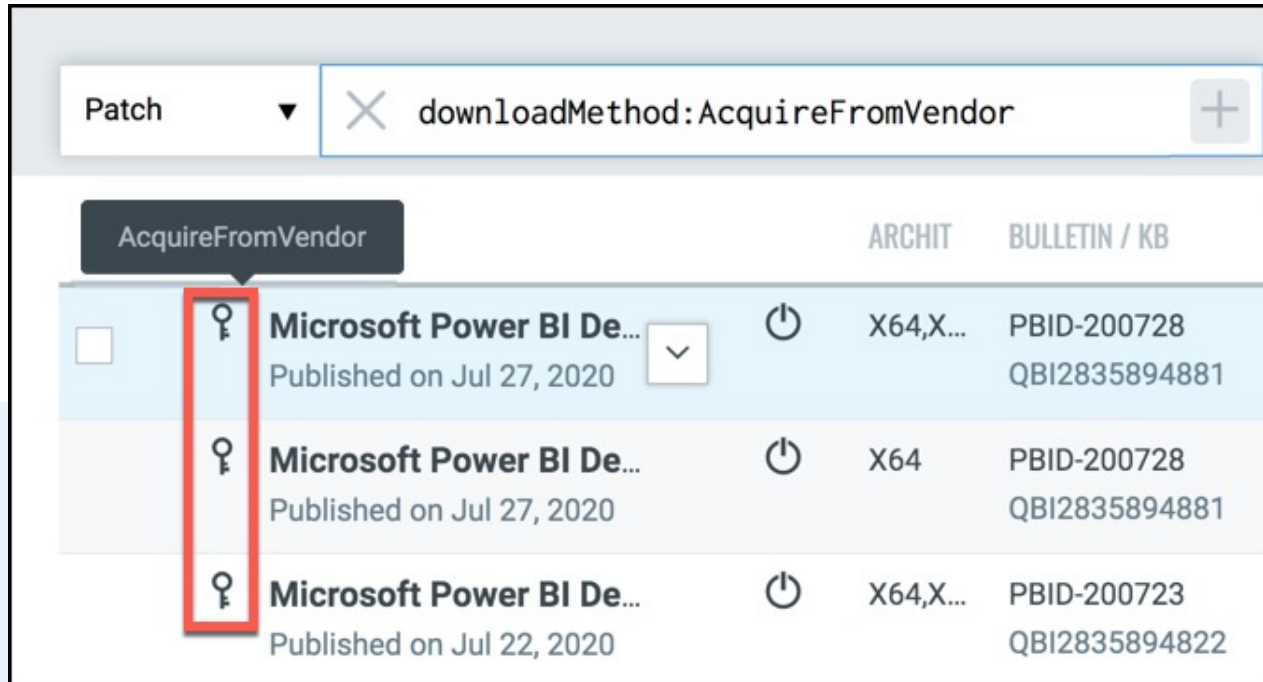
Catalog's Default Display Filters









A screenshot of a web application's filter menu. At the top, there is a tab labeled 'Filters' with a dropdown arrow and a small blue circle containing the number '2'. Below the tab, the menu is divided into two sections. The first section is titled 'Patch Status' and contains two options: 'Missing' with a checked checkbox and 'Installed' with an unchecked checkbox. The second section is titled 'Only Latest Patches (Non-superseded)' and contains one option: 'Yes' with a checked checkbox.

- The default filters in the Patch Catalog, display patches that are missing and only the latest patches (non-superseded).

Acquire From Vendor



Patch ▼ ✕ downloadMethod:AcquireFromVendor +

	AcquireFromVendor		ARCHIT	BULLETIN / KB
<input type="checkbox"/>	 Microsoft Power BI De... Published on Jul 27, 2020 ▼		X64,X...	PBID-200728 QBI2835894881
	 Microsoft Power BI De... Published on Jul 27, 2020		X64	PBID-200728 QBI2835894881
	 Microsoft Power BI De... Published on Jul 22, 2020		X64,X...	PBID-200723 QBI2835894822

- Patches identified with the “key-shaped” icon, cannot be downloaded by Qualys’ Cloud Agent.



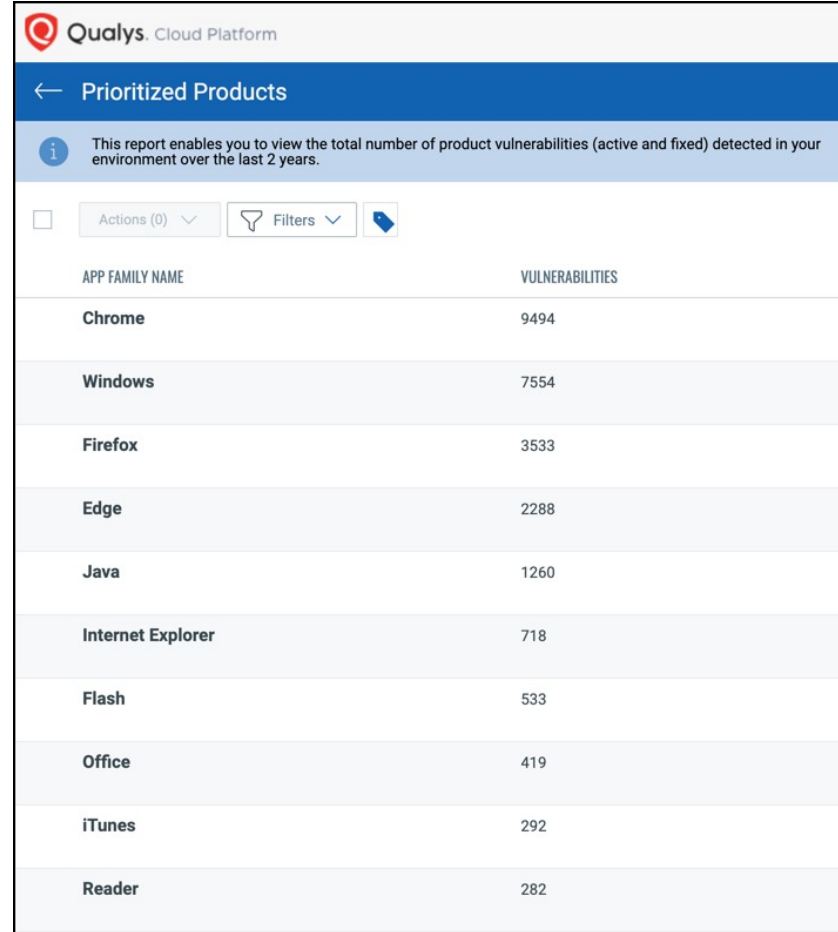
Prioritized Products

Prioritized Products

- Automate the selection of patches in recurring deployment jobs
- Patches are selected using QQL
- Patches meeting the query condition are included in scheduled deployment jobs (daily, weekly, monthly)
- Patch Jobs are initiated from the Patch Catalog (i.e., click the “Prioritized Products” button).

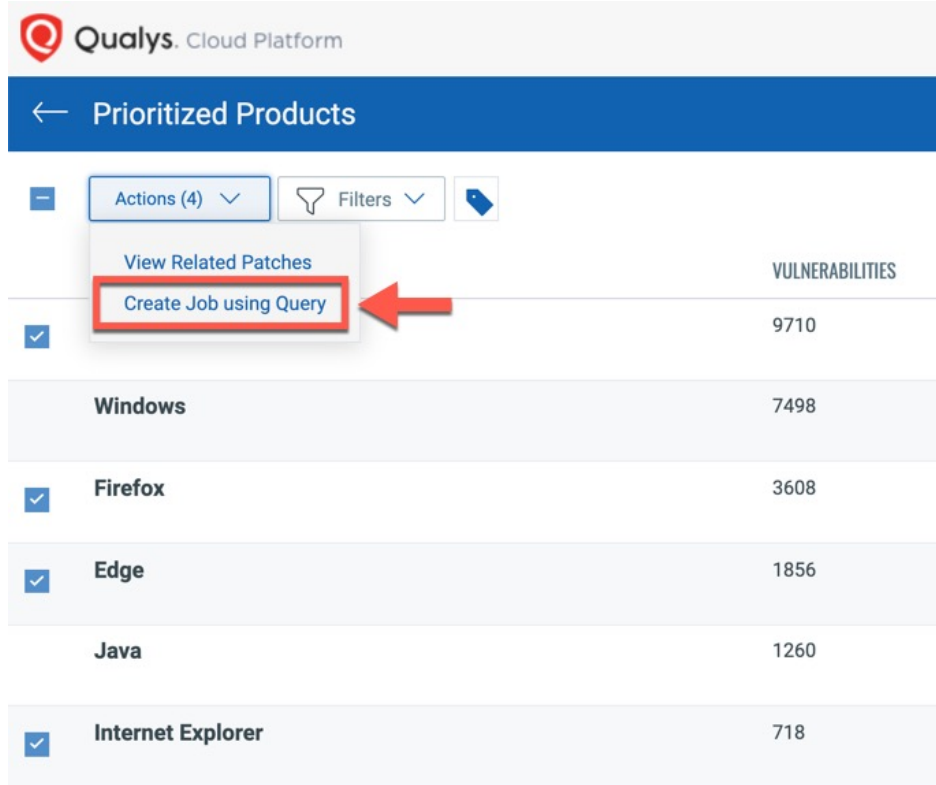
Prioritized Products

- Products listed near the top, introduce the most vulnerabilities into your business and enterprise architectures.



APP FAMILY NAME	VULNERABILITIES
Chrome	9494
Windows	7554
Firefox	3533
Edge	2288
Java	1260
Internet Explorer	718
Flash	533
Office	419
iTunes	292
Reader	282

Create Job Using Query



The screenshot shows the Qualys Cloud Platform interface. At the top, there's a header with the Qualys logo and 'Qualys. Cloud Platform'. Below it, a blue bar contains a back arrow and the text 'Prioritized Products'. Underneath, there's a section with 'Actions (4)' (a dropdown menu), 'Filters' (a dropdown menu), and a tag icon. The 'Actions (4)' menu is open, showing two options: 'View Related Patches' and 'Create Job using Query'. The 'Create Job using Query' option is highlighted with a red box, and a red arrow points to it. Below the menu, there's a table with the following data:

	VULNERABILITIES
<input checked="" type="checkbox"/> [Application Name]	9710
Windows	7498
<input checked="" type="checkbox"/> Firefox	3608
<input checked="" type="checkbox"/> Edge	1856
Java	1260
<input checked="" type="checkbox"/> Internet Explorer	718

- Select applications from the “Prioritized Products” list and use the “Actions” button to “Create Job using Query.”
- A query designed to target the selected applications is constructed automatically (using QQL).

Create a Query for Patches

Select Patches

Choose the patches you want to install for the selected assets or create a query for the job.

☐ Select Patches ☒ Create a Query for Patches

Patch ▼ ✕

appFamily:`Chrome` or appFamily:`Firefox` or appFamily:`Edge` or appFamily:`Internet E ↕ ?

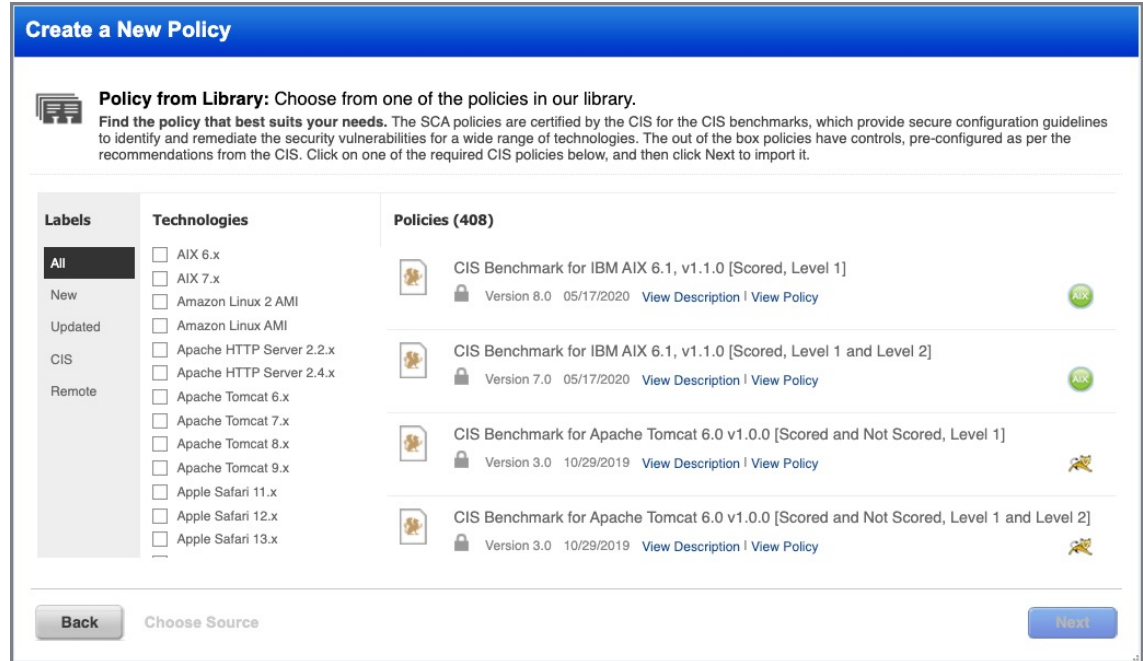
Note: For optimum performance, only missing and non-superseded patches that match the QQL criteria will be added to the job.

- The generated query condition(s) will specify the criteria for selecting patches each time the job runs (daily, weekly, monthly).

Additional VMDR Applications







Security Configuration Assessment (SCA)

- Monitor and assess assets for misconfigurations.
- Leverage **Qualys Scanners and Agents**.
- Provides over 400 CIS Benchmark Policies for hundreds of OS and application technologies.
- Upgrade from SCA to PC.



CloudView & Cloud Security Assessment (CSA)

- Leverage **Qualys Cloud Connectors**.
- Add cloud-based assets to your asset inventory.
- Collect metadata to assess both your account and assets for misconfigurations.
- CSA provides “out-of-box” policies for your AWS, Azure, and Google accounts.

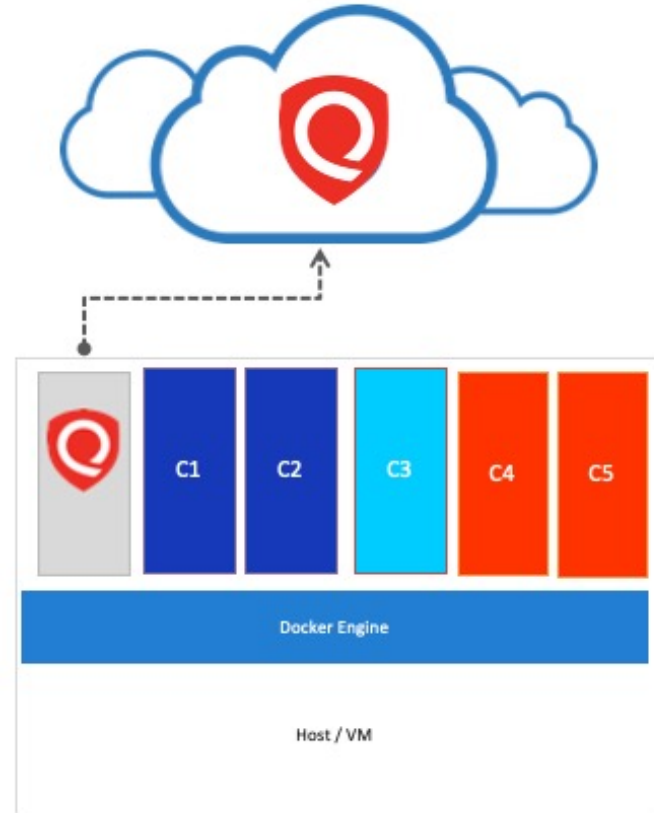
Azure Function App Best Practices Policy	
AWS Best Practices Policy	
GCP Best Practices Policy	
GCP Cloud Functions Best Practices Policy	
CIS Amazon Web Services Foundations Benchmark	
Azure Best Practices Policy	

Container Security (CS)

- Assess container applications for vulnerabilities and misconfigurations.
- Deploy **Container Sensors** right along side other container applications.

Container Sensor Types:

1. General Sensor
2. Registry Sensor
3. CI/CD Pipeline Sensor



CertView (CERT)

Leverage **Qualys Scanner Appliances** to provide visibility into certificates across your network and enterprise architecture (on-premise and cloud-based).

- Create a baseline inventory of existing certificates and monitor for new certificates.
- Identify certificates that have weak signatures or key lengths and Certificate Authorities that have not been vetted or approved.
- Certificate grades allow administrators to quickly assess server SSL/TLS configurations.
- Certificate Renewals prevent expired and expiring certificates from interrupting critical business functions.

Monitored

Archived

Actions (1) ▾

New ▾

1 - 9 of 9

◀

▶

⬇

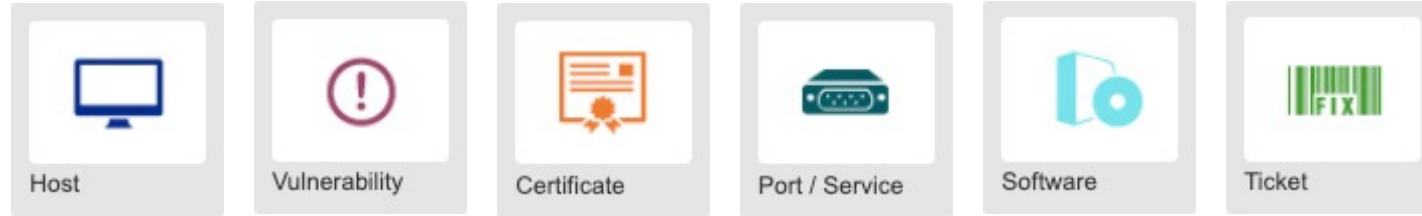
↺

📄

⚙

NAME/ORGANIZATION ↑	EXPIRATION	LAST FOUND	INSTANCES	ASSETS
TRN-WIN10-PRO.trn.qualys.com	Apr 04, 2022	Oct 17, 2021	1	1
<div><div><div><div>✓</div></div></div>TRN-WIN10.trn.qualys.co</div>	<div>Nov 17, 2021</div> <div>in 30 days</div>	Oct 17, 2021	1	1
<div>demo1.vmtest.me</div> <div>vmtest</div>	Jan 06, 2025	Oct 17, 2021	2	1
<div>demo1.vmtest.me</div>	<div>Aug 25, 2016</div> <div>5 year(s) ago</div>	Oct 17, 2021	4	2
trn-win2012-dc.trn.qualys.com	Nov 18, 2021	Sep 10, 2021	1	1
win10dfw220	Jul 17, 2021	Apr 21, 2021	1	1

Continuous Monitoring



- Add custom alerts to your vulnerability assessment program for immediate response.
- CM works in tandem with VM/VMDR:
 - Deploy **Qualys Scanner Appliances** and/or activate the VM module for deployed **Qualys Agents**.
 - Schedule frequent or continuous vulnerability scans.

VMDR for Mobile Devices



- Collect inventory and configuration data from your mobile devices (integration with Qualys Global AI).
- Perform vulnerability and compliance assessments.
- Perform active device operations, like locking a screen or locating a missing device.

Following This Course

VMDR Certification Exam

<https://gm1.geolearning.com/geonext/qualys/scheduledclassdetails4enroll.geo?&id=22511237824>

VMDR Course Survey

<https://forms.office.com/r/rsy0Aja6Xz>

VMDR Trial Account

<https://www.qualys.com/forms/vmdr/>



Qualys.

Thank You

training@qualys.com